CEBEO INDUSTRY • Winter 2025 • Jaargang 6• Editie 10

CEBEO

INDUSTRY

NIS2 ONTSLEUTELD:
WAT DE NIEUWE VERPLICHTINGEN VOOR JOU BETEKENEN

HOME & BUILDING | INDUSTRY

WETGEVING
In 7 stappen naar sterke cyberbeveiliging

PREVENTIE
IEC 62443-standaard als leidraad

OPPORTUNITEIT
NIS2 biedt extra kansen voor machinebouwers

cebeo
A Sonepar Company

10

EDITIE

Een uitgave van
CEBEO NV

MAATSCHAPPELIJKE ZETEL:
Eugène Bekaertlaan 63, 8790 Waregem

VERANTW. UITGEVER:
Régis André
Eugène Bekaertlaan 63, 8790 Waregem

HOOFDREDACTIE:
Summer Vanhaverbeke

REDACTIE:
Bart Vancauwenberghe

SECRETARIAAT:
Julie Delannay

VERTALING FRANSE EDITIE:
Yamagata Europe

VORMGEVING:
Remark Reclame

DRUK:
GBL, Kortrijk

BESTE LEZER

De door de Europese Unie ingevoerde NIS2-richtlijn (Network and Information Security Directive 2) is voor de industrie van cruciaal belang omdat het de digitale weerbaarheid versterkt en cyberdreigingen vermindert.
In een tijd waarin cyberaanvallen toenemen, biedt deze richtlijn een juridisch kader dat bedrijven verplicht hun cybersecuritymaatregelen te verbeteren.

Bedrijven die kwetsbaar zijn voor cyberaanvallen lopen het risico op datalekken, productieonderbrekingen en financiële verliezen. Door te voldoen aan NIS2 versterken bedrijven hun verdediging tegen aanvallen en bouwen ze vertrouwen op bij klanten en partners.

Daarnaast stimuleert de richtlijn samenwerking binnen en tussen sectoren. Het verplicht bedrijven om incidenten te melden en informatie over dreigingen te delen, wat leidt tot snellere respons en betere preventie. Ook wordt de toeleveringsketen veiliger, omdat alle betrokken partijen aan strikte normen moeten voldoen.

Voor bedrijven in essentiële sectoren, zoals energie, gezondheidszorg en transport, is NIS2 niet alleen een verplichting, maar vooral een strategisch voordeel. Door proactief te voldoen, versterken ze hun concurrentiepositie en bewijzen ze te beantwoorden aan de groeiende eisen van een digitaal verbonden (productie-)wereld. Daarom doet de industrie er goed aan NIS2 vooral als een noodzakelijke investering in de toekomst te beschouwen.

In dit magazine staan we uitgebreid stil bij de meerwaarde van NIS2 en hoe verschillende fabrikanten hun eindklanten helpen eraan te voldoen. Hoewel Cebeo zelf niet NIS2-plichtig is, spreekt het voor zich dat we alles in het werk stellen om zelf een zo hoog mogelijk niveau van cybersecurity te bereiken. Ook daarover geven we een extra woordje uitleg.

Veel leesplezier!

Summer Vanhaverbeke
Communications Coordinator

NIS2 ONTSLEUTELD: WAT DE NIEUWE VERPLICHTINGEN VOOR JOU BETEKENEN

INHOUD

6

DIRK DE PAEPE (CCB) :

"Het kleinste hiaat in je digitale beveiliging is voor cybercriminelen genoeg om toe te slaan."

KOEN PAUWELYN (SIEMENS) :

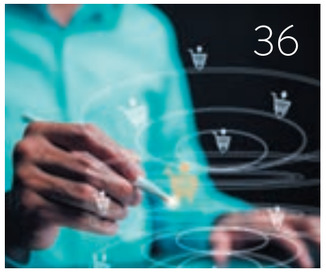
"We gaan uit van een gefaseerde aanpak met een aantal duidelijke prioriteiten."

PETER-JAN DELTOUR (PHOENIX CONTACT):

"Het komt erop aan een goede balans te vinden tussen investeren in cyberveiligheid en operationele efficiëntie.."

THOMAS VASEN (HMS) :

"De voorgestelde normen in de IEC 62443-standaard helpen effectief om naar veiliger industriële processen te evolueren."



FLORIAN DELANGHE (CEBEO) :

"Voor de bescherming van kritische data en de bedrijfszekerheid, is 'edge computing' heel nuttig."

32

STEVEN DEPUYDT (CEBEO) :

"Het grootste gevaar loert om de hoek bij onvoorzichtige IT-handelingen van je eigen medewerkers."

CENTRE FOR
CYBERSECURITY BELGIUM

VOLDOEN AAN NIS2-WETGEVING MOET VOOR TALRIJKE ENTITEITEN EEN PRIORITEIT ZIJN

Een cyberaanval is de overtreffende trap van online kwetsbaarheid: daar kan je je maar beter optimaal tegen wapenen. Dat is ook de bedoeling van de nieuwe Belgische NIS2-wetgeving, die sinds 18 oktober operationeel is geworden. Wat houdt dit precies in? Hoe kan je eraan voldoen? Welke risico's loop je als je er niét aan voldoet? Dirk De Paepe, Senior Certification Expert bij het CCB (Centre for Cybersecurity Belgium) legt alles bevattelijk uit.

Lees verder op pagina 8

"Cybersecurity is een absolute must geworden"

Vervolg van pagina 7

Europa heeft in 2016 een richtlijn voor cybersecurity uitgevaardigd, die alle lidstaten in wetgeving moe(s)ten omzetten. Dat heeft in België op 7 april 2019 geleid tot de NIS-wet (NIS staat voor 'Network and Information Systems', red.).

"De Europese NIS-richtlijn had drie doelstellingen", stipt Dirk De Paepe aan. "Ze verplichtte de nationale overheden tot het spenderen van de nodige aandacht aan cybersecurity. Ten tweede moest het de Europese samenwerking tussen cybersecurity-autoriteiten versterken. Daarnaast moest ze ook de belangrijkste operatoren in de meest cruciale sectoren verplichten tot het nemen van veiligheidsmaatregelen en het melden van incidenten."

Dirk De Paepe, Senior Certification Expert bij het CCB

VERHOOGDE NOODZAAK

NIS1 slaagde er evenwel niet in alle vooropgezette doelstellingen af te vinken. "Het leverde overal in Europa wel positieve resultaten op, maar het toepassingsgebied was te beperkt en er was nogal wat onduidelijkheid over de doelgroep voor wie NIS1 van kracht was. Dat leidde tot een inefficiënte toepassing en dito sanctionering. Daarnaast stelde Europa te grote verschillen vast in de manier waarop de lidstaten dit benaderden. Bovendien is de noodzaak aan cybersecurity fors gegroeid. Dat komt door een gevoelige stijging van de cybercriminaliteit, wat zich reflecteert in een aanzienlijke toename van het aantal dreigingen. Daarnaast is onze integrale maatschappij veel afhankelijker van de digitale wereld geworden en is er veel meer connectiviteit, wat de kwetsbaarheid verhoogt."

"We merken nu al dat veel andere lidstaten België als voorbeeld nemen."

Safeonweb.be

Daarom kwam Europa met een verstrengde opvolger – NIS2 – op de proppen. "Die behoudt dezelfde doelstellingen als NIS1, maar breidt het aantal entiteiten en sectoren die tot de doelgroep behoren enorm uit. Daarnaast omvat ze meer duidelijke maatregelen, uitgebreidere regels rond incidentmelding, strengere en specifiekere sanctieregels én een sterke responsabilisering van het topmanagement van elke entiteit."

PIONIER

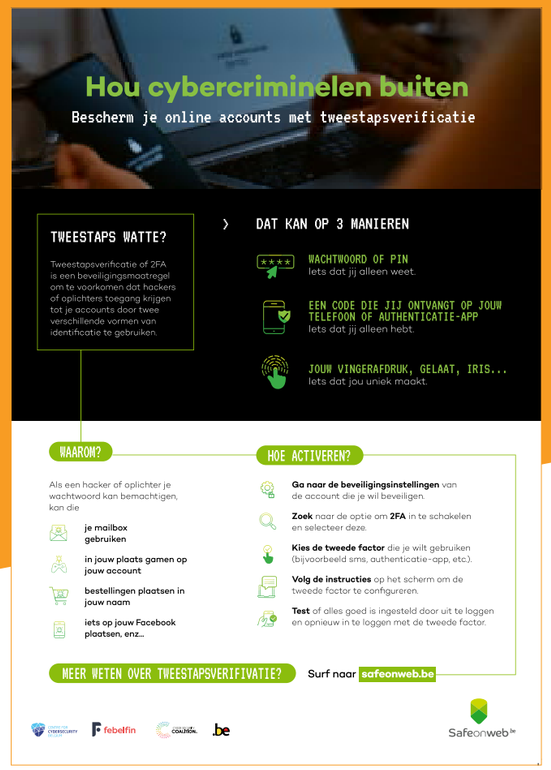
België nam die nieuwe richtlijn heel ernstig en is zelfs de eerste om die volledig te vertalen naar de nieuwe NIS2-wetgeving, die op 18 oktober 2024 in voege is getreden. "Het is ronduit goed nieuws dat de overheid veel belang hecht aan die wetgeving en de uitvoerende besluiten die daarmee gepaard gaan. We merken nu al dat talrijke andere lidstaten België als voorbeeld nemen. Daarvan zijn er een aantal geneigd om onze aanpak naar hun land te kopiëren, wat voor onze ondernemingen een voordeel zou kunnen zijn. Het CCB was bepalend bij de opstelling van de NIS2-wet en voerde daarover ook overleg met belangenorganisaties en sectorale overheden."

Lees verder op pagina 10

7-STAPPENPLAN

Wat moet je als entiteit nu doen in het NIS2-verhaal? Daarvoor werkte het CCB een zevenstappenplan uit, waarvan je de uitgebreide versie online kan vinden.

"Voor essentiële en belangrijke bedrijven is het cruciaal om ook hun toeleveringsketen te beveiligen."



Campagnemateriaal © Safeonweb 2024

Het controleren van de genomen maatregelen met betrekking tot cyberbeveiliging, gebeurt door conformiteitsbeoordelingsinstellingen (CAB's). Dat zijn door het CCB geautoriseerde organisaties, die online staan opgelijst (www.cyfun.be), net als de voorwaarden om zo'n CAB te kunnen worden.

"Voor 'belangrijke' entiteiten zijn regelmatige conformiteitsbeoordelingen in principe vrijwillig. Voor 'essentiële' bedrijven daarentegen, zijn die regelmatige conformiteitsbeoordelingen verplicht. Essentiële entiteiten zijn door de band genomen grote organisaties in zeer kritieke sectoren en zijn levensbelangrijk voor een land: als die omwille van een cyberaanval niet meer functioneren, hebben erg veel mensen daar last van.

Nutsmaatschappijen of ziekenhuizen zijn daar goede voorbeelden van. Belangrijke bedrijven (bijvoorbeeld koerierdiensten) zijn door de band genomen middelgrote organisaties in de zeer kritieke sectoren en grote en middelgrote organisaties in andere kritieke sectoren waar cyberincidenten eveneens grote gevolgen voor de samenleving kunnen hebben.
Daarnaast is het voor essentiële en belangrijke bedrijven cruciaal om ook hun toeleveringsketen te beveiligen. Je mag dus concluderen dat NIS2 op veel entiteiten een forse impact zal hebben."

SANCTIES

Je als entiteit niets van NIS2 aantrekken? Geen goed idee. Ten eerste schiet je jezelf in de voet door cybersecurity achteloos achterwege te laten, bovendien gaat het ook om een wetgeving: je moét je daar dus wel aan houden.

"Wie er niet aan voldoet en dus inbreuken pleegt inzake risicobeheersmaatregelen of incidentmeldingen, riskeert in eerste instantie administratieve maatregelen, zoals waarschuwingen en bindende instructies. Als een essentiële entiteit eraan verzaakt, kan iemand met leidinggevende verantwoordelijkheden, zoals bijvoorbeeld een algemeen directeur, zelfs een tijdelijk verbod op het uitoefenen van zijn functie in die entiteit krijgen."

Ook forse geldboetes zijn mogelijk. "Voor belangrijke entiteiten kunnen die oplopen tot 7 miljoen euro, of 1,4% van de totale wereldwijde omzet in het voorafgaande boekjaar (afhankelijk van welk bedrag hoger is). Bij essentiële entiteiten kan dat oplopen tot 10 miljoen euro, of 2% van die omzet (afhankelijk van welk bedrag hoger is)."

Lees verder op pagina 11

Vervolg van pagina 9

Het CCB heeft de afgelopen weken en maanden kosten noch moeite gespaard om iedereen zo goed mogelijk te informeren. "Dat deden we via tientallen presentaties, video's waarin we de fundamentele basis voor cybersecurity zo goed mogelijk hebben uitgelegd en via onze website.

Daarnaast maken we er een erezaak van om elke vraag naar informatie die ons via mail bereikt, één op één te beantwoorden. Uiteraard hebben we ook de sectorfederaties en werkgeversorganisaties uitgebreid met informatie bevoorraad. Ondanks al die inspanningen, stellen we vast dat talrijke organisaties en ondernemingen het nog in Keulen horen donderen als de NIS2-wetgeving ter sprake komt. Daarom zetten we onze infocampagnes de komende maanden onverminderd verder."

ESSENTIEEL VERSUS BELANGRIJK

In België maakt men het onderscheid tussen belangrijke en essentiële bedrijven. De uitleg over hoe dat onderscheid wordt gemaakt, vind je op de website van het CCB en is bepaald in bijlage I en bijlage II van de Belgische NIS2-wet.

"Wie er niet aan voldoet, riskeert geldboetes of een tijdelijk verbod op het uitoefenen van zijn functie."

Dirk De Paepe, Senior Certification Expert bij het CCB

Vervolg van pagina 11

AAN DE SLAG

Er is dus geen tijd te verliezen om met NIS2 aan de slag te gaan. Dirk De Paepe raadt entiteiten in eerste instantie aan om te starten met CyberFundamentals Basis. “Dat gaat bijvoorbeeld om het maken én controleren van back-ups: je bent niets met back-ups die op hetzelfde netwerk draaien en/of met back-ups die niet functioneren. Daarnaast is het heel verstandig om Multi-Factor Authenticatie (MFA, methode die de identiteit van de gebruiker op meer dan één manier verifieert, red.) te integreren. Wie hier niet over beschikt, loopt sowieso een grotere kans om het slachtoffer van cybercriminelen te worden. Die hebben vaak aan het kleinste hiaat in cyberbeveiliging voldoende om toe te slaan en richten zich zowel op grote als kleine bedrijven.”

Met de ‘scoping tool’ in de snelstartgids op de website van het CCB (www.cyfun.be) kan elke entiteit nagaan of ze belangrijk, dan wel essentieel is. De CyFun®-zelfevaluatietool op diezelfde website geeft je als organisatie een duidelijk idee wat het niveau van je cyberweerbaarheid is en laat je toe te plannen en budgetteren op welke manier je die cyberweerbaarheid kan verhogen om uiteindelijk te voldoen aan de wettelijke vereisten van NIS2.

www.cyfun.be

www.safeonweb.be

Campagnemateriaal © Safeonweb 2024

CEBEO PARTNERSHIPS SIEMENS

NIS2-conform zijn is een uitdaging die razend actueel is voor heel wat industriële bedrijven. Dat gaat gepaard met noodzakelijke aanpassingen op IT-niveau, maar zeker ook op vlak van operationele technologie (OT). Cybersecurity is een thema waar Siemens intern én extern heel wat aandacht aan besteedt. Drie specialisten duiden hoe de technologiespeler de industriële eindklant hierin begeleidt.

Lees verder op pagina 16

“Cybersecurity vergt inspanningen op diverse niveaus”

SIEMENS ONDERSTEUNT INDUSTRIËLE EINDKLANTEN OM NIS2-CONFORM TE ZIJN

“Netwerksegmentatie is een belangrijke stap, onder meer voor het beveiligen van verouderde machines.”

Gregory Putman, Sales Specialist industriële communicatie voor Wallonië

Vervolg van pagina 15

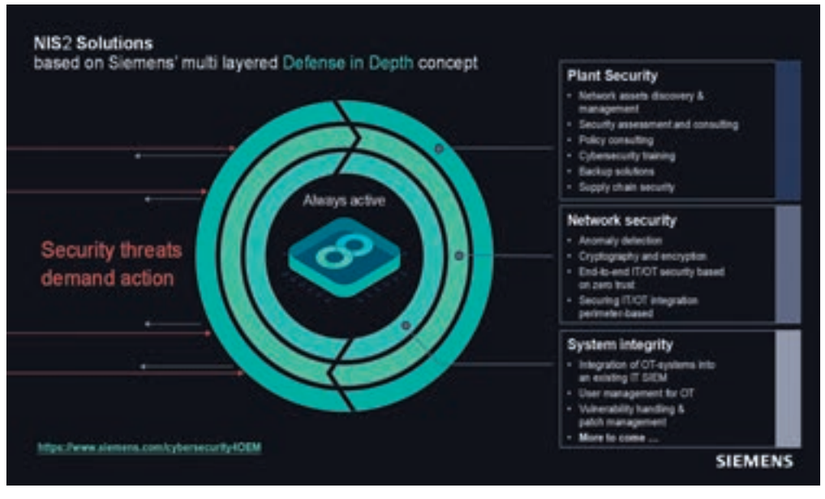
“Uiteraard is cybersecurity voor Siemens een topprioriteit”, opent Koen Pauwelyn, Service Sales Specialist en vanuit die functie ook intens bezig met cybersecurity. “IT- en OT-apparatuur die volledig veilig zijn, is een vereiste die heel wat van onze klanten terecht in hun lastenboeken opnemen. Onze services en productportfolio zijn in die zin enorm geëvolueerd. We willen een voortrekkersrol spelen, onder meer door klanten gericht te informeren.”

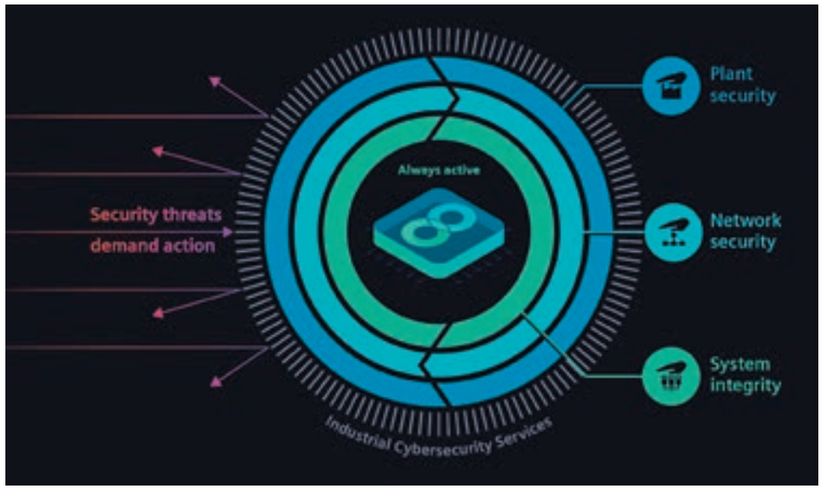
Dat is ook nodig, weet zijn collega Bart Boumans (Sales Specialist industriële communicatie voor Vlaanderen). “We maken het nog geregeld mee dat klanten die tegen medio 2025 NIS2-geregistreerd moeten zijn, het in Keulen horen donderen. Dat geldt evenzeer voor bedrijven die ervan overtuigd zijn niets met NIS2 te maken te hebben. Nochtans: als zij een leverancier zijn van een onderneming die wél ‘NIS2 compliant’ moet zijn, doen ze er goed aan toch de nodige inspanningen te doen, omdat NIS2-plichtige ondernemingen de taak hebben hun ‘supply chain’ eveneens veilig te stellen.”

Bij Siemens merken ze vaak dat industriespelers zich bij NIS2 vooral op IT focussen, maar de OT-zijde verdient minstens evenveel aandacht. “PLC’s, sensoren, machines,… moeten eveneens beveiligd zijn”, gaat Koen Pauwelyn verder. “Dat is uitdagend, vermits machines veel langer meedraaien dan pakweg een laptop en vaak nog werken met verouderde systemen die niet meer up te daten zijn. Zelfs als ze wél op moderne technologie draaien, is er jaarlijks doorgaans maar één keer de mogelijkheid om ze te ‘patchen’, vermits ze de klok rond werken en een bedrijf het zich niet kan permitteren om om de haverklap de productie stil te leggen in functie van updates.”

PLAN VAN AANPAK

Het is dus vijf voor twaalf om een coherente strategie uit te werken en uit te voeren. Siemens kan in dat verhaal een cruciale rol vertolken. Koen: “Voor een systeemintegrator is het moeilijk om zijn eigen realisaties te beoordelen op vlak van cybersecurity. Wij kunnen die rol, als derde partij, voor onze rekening nemen. Daarbij starten we met een nulmeting, die de huidige situatie in beeld brengt. Op basis daarvan kunnen we een ‘roadmap’ uitwerken die alle vereiste aanpassingen in kaart brengt om aan de NIS2-richtlijn te beantwoorden. Omdat het onmogelijk is om alles in één keer te wijzigen, gaan we uit van een gefaseerde aanpak met een aantal duidelijke prioriteiten.”





INTERACTIE MET CEBEO

De wisselwerking tussen Cebeo en partners zoals Siemens, kan een meerwaarde betekenen in de uitdaging van de industrie om NIS2-conform te zijn. Gregory: “Cebeo maakt zijn klanten duidelijk wat NIS2 precies is en fungeert als een gids die hen wegwijs maakt in de te nemen stappen. Siemens kan voor de juiste informatie en opleidingen zorgen en vervolgens ook voor de begeleiding om NIS2 binnen de organisatie uit te rollen.”

Siemens bekijkt cybersecurity in verschillende lagen, volgens het ‘Defense in Dept’-concept. Een eerste laag is netwerksecurity. “Netwerksegmentatie is een belangrijke stap, onder meer voor het beveiligen van verouderde machines”, verduidelijkt Gregory Putman (Sales Specialist industriële communicatie voor Wallonië). “Ook het voorzien van firewalls voor dergelijke machines is een ideale manier om ze te beveiligen, zodat ze geïsoleerd zijn van de rest van het OT-park.”

System integrity is een tweede essentiële pijler. “Dat kan onder meer via TIA Portal (Total Integrated Automation Portal), een softwareplatform waarmee je automatiseringsproducten, zoals PLC’s, eenvoudig én veilig kunt programmeren met gebruik van geëncrypteerde communicatie.

Lees verder op pagina 18

Bart Boumans, Sales Specialist industriële communicatie voor Vlaanderen

“NIS2-plichtige ondernemingen hebben de taak ook hun ‘supply chain’ veilig te stellen.”

“Het is cruciaal af en toe te testen hoe goed back-ups werken.”

Koen Pauwelyn, Service Sales Specialist

Vervolg van pagina 17

TIA portal is onder meer uitgerust met een usermanagementsysteem, waarbij je duidelijk kan bepalen wie waarvoor bevoegd is. Dit laat ook toe om vanuit het IT-systeem Active Directory (AD) het gebruikersmanagement te bepalen voor de OT-toestellen.

‘Anomaly detection’ is eveneens cruciaal. Dit is een geavanceerde cybersecuritybenadering die real-time bescherming biedt door automatisch verdachte activiteiten te detecteren, te analyseren en te melden.”

PLANT SECURITY

Ook op plant security kan je als bedrijf maar beter goed inzetten. “Dit omvat onder meer het accuraat afschermen van je infrastructuur van de buitenwereld. Plant security op de juiste manier aanpakken, begint met het correct informeren van je medewerkers, onder meer door hen te laten deelnemen aan algemene opleidingen over cybersecurity.

We merken dat opleidingen vaak een besparingspost zijn voor bedrijven, maar op (lange) termijn kan dat negatieve gevolgen voor de productiviteit hebben. Ook meer gerichte cybersecurity-opleidingen, bijvoorbeeld over engineeringprogramma’s, geven vaak inzichten in complexe materie die onvoldoende bekend is.”

100% cybersecurity bestaat niet, maar met adequate monitoring kan je veel onheil vermijden. “De integratie van alarmsystemen die anomalieën detecteren, is een stap in de goede richting. Deze oplossingen monitoren je netwerk op een passieve manier: als ze een alarm hebben uitgestuurd, beslis je zelf welke acties je uitvoert.”

Bij Siemens raden ze eindklanten aan om werk te maken van de juiste firmware (met de gratis security-updates voor PLC’s en andere OT-componenten) en aan verstandig back-up-management te doen. “Ook dat is een belangrijke pijler binnen NIS2. Het is essentieel om dankzij back-ups data te kunnen recupereren en af en toe daadwerkelijk te testen hoe goed die back-ups werken.

Elk bedrijf moet werk maken van een duidelijk ‘disaster plan’, met duidelijke maatregelen die in geval van een probleem snel in actie kunnen treden. Daarvoor moet je een verantwoordelijke aanduiden, die ervoor zorgt dat de vastgelegde procedures nauwkeurig worden opgevolgd en die protocollen idealiter ook regelmatig test.”

INFO

Ontdek hier meer van Siemens over NIS2:

CEBEO PARTNERSHIPS
PHOENIX CONTACT

PHOENIX CONTACT RAADT INDUSTRIE AAN OM INVESTERING IN CYBERSECURITY PRIORITEIT TE MAKEN

Je wil het niet meemaken dat je productie door externe factoren van vandaag op morgen helemaal stilvalt. Nochtans bestaat dat risico wel als je nonchalant met cybersecurity omgaat. Bij Phoenix Contact breken ze dan ook terecht een lans om hier echt werk van te maken. “Je hoeft niet in ijltempo van 0 naar 100 te schakelen: ook de ontwikkeling van juiste procedures en het aanpassingsproces van je medewerkers vergen tijd”, klinkt het bij Peter-Jan Deltour, Head of OT & Cybersecurity bij Phoenix Contact België.

Lees verder op pagina 22

“Preventiekost ligt stukken lager dan prijs van een cyberaanval”

“Lang niet elke geslaagde cyberaanval op een kmo komt in het nieuws.”

Vervolg van pagina 21

Peter-Jan Deltour, Head of OT & Cybersecurity bij Phoenix Contact België

Als toonaangevend technologiebedrijf biedt Phoenix Contact innovatieve oplossingen voor elektrotechniek en automatisering. Je vindt hen overal waar sprake is van het verbinden, het verdelen of het aansturen van stroom of datastromen. Daarvoor ontwikkelt en produceert het bedrijf producten zoals klemmenstroken, voedingen, PLC’s en IoT-oplossingen, gericht op sectoren als machinebouw, energie en infrastructuur. Phoenix Contact helpt bedrijven efficiënter en veiliger te werken, steeds met oog voor duurzaamheid en een focus op digitalisering.

CYBER RESILIENCE ACT

“Dat veiligheidsaspect wordt almaar belangrijker”, onderstreept Peter-Jan Deltour. “Onze producten moeten voldoen aan industriële vereisten voor cybersecurity. Tegen 2027 dienen ze ook te beantwoorden aan de normen van de Cyber Resilience Act, die zich vooral op componentenleveranciers – zoals wij – richt. Die nieuwe Europese richtlijn accentueert nogmaals de enorm gestegen noodzaak aan het krachtdadig beveiligen van IT- en OT-oplossingen.”

Bij het integreren van cybersecurity in zijn oplossingen, neemt Phoenix Contact de standaard IEC 62443 als leidraad. “Dit is één van de weinige cybersecurity-standaarden die zich ook op de industriële markt focust. Als onze systemen bij industriële eindklanten worden geïnstalleerd, moeten ze gedurende hun volledige levensduur – dus ook nog binnen pakweg 20 jaar – optimaal functioneren en ook op het eind van die termijn nog aan de veiligheidsvereisten voldoen. IEC 62443 behartigt dat vanuit een integraal luik over componentbeveiliging en -veiligheid. Onze PLC’s beantwoorden al sinds 2019 aan die vereisten, sindsdien gebeurt de integratie stelselmatig ook in al onze andere productgroepen.”

Het cybersecurityverhaal tot de exclusieve verantwoordelijkheid van je IT-afdeling uitroepen, kan risicovol zijn. “Vaak weten die mensen niet voldoende gedetailleerd wat er zich zoal afspeelt inzake operationele technologie. Daarom is het een goed idee om dat toe te vertrouwen aan een partner met diepgaande kennis, zoals bijvoorbeeld een leverancier van dergelijke componenten.”

VERPLICHTE AUDIT

Naast het beveiligen van het eigen productportfolio, biedt Phoenix Contact ook services aan om de eindklanten bij te staan bij het uitstippelen en implementeren van cybersecurity. Vele ondernemingen beseffen dat ze een gestructureerde cybersecurity-aanpak nodig hebben voor hun OT, maar vaak weten ze niet hoe hieraan te beginnen. Om industriële eindklanten te helpen bij het cyberveilig maken van hun infrastructuur, gaat Phoenix Contact heel planmatig te werk.

“Ten eerste brengen we alle elementen (machines, fabriekshal,…) volledig in kaart. De documentatie die bedrijven op dat vlak ter beschikking stellen, komt in de meeste gevallen niet 100% overeen met de realiteit. Als ondernemingen onze ondersteuning willen, is die audit dan ook verplicht, want we moeten zo nauwkeurig mogelijk weten wat we precies moeten beveiligen.”

Lees verder op pagina 24

Vervolg van pagina 23

Stap twee is een risicoanalyse. “Niet op cybersecurity inzetten, is een grote fout. Te snel werken is evenmin een goed idee. De technologie op zich kost geld, maar je moet intussen ook procedures laten mee evolueren en je medewerkers de tijd geven om vertrouwd te raken met de nieuwe aanpak. Een te strak tempo aanhouden kan ertoe leiden dat mensen niet meer mee zijn, waardoor er een omgekeerd effect ontstaat en het risico zo mogelijk nog groter wordt. Je mensen zullen ongetwijfeld de beste bedoelingen hebben, maar het is de realiteit dat ze in dergelijke processen in vele gevallen de zwakste schakel zijn.”

Het resultaat van die risicoanalyse is een lijst die alle kleinere en grotere pijnpunten in beeld brengt. “Vervolgens is het aan het bedrijf zelf om de belangrijkste prioriteiten aan te duiden en een timing op te stellen om die aan te pakken. Sowieso kan je wel beginnen met een aantal ‘quick wins’, zoals een correcte configuratie van de firewalls. Andere maatregelen moet je echt concreet inplannen, vermits die een impact kunnen hebben op de operationele stroom van je organisatie.

INCIDENTGEDREVEN VRAAG

Je kan het je eigenlijk niet langer permitteren om cyberveiligheid niet hoog op de agenda te zetten, vindt Peter-Jan. “We merken gelukkig een groeiende vraag van bedrijven om hen daarbij te ondersteunen, maar helaas gebeurt dat nog (te) vaak nadat ze al met een incident geconfonteerd werden, of nadat een cyberaanval bij een bedrijf veel media-aandacht heeft gekregen. Weet dat die meldingen maar het topje van de ijsberg zijn: lang niet elke geslaagde cyberaanval op een kmo komt in het nieuws.”

Akkoord, cybersecurity is een kost, maar het prijskaartje van preventie ligt sowieso aanzienlijk lager dan de kosten die je moet ophoesten om de impact van een aanval zo veel mogelijk te beperken. “Bovendien is de vraag niet zozeer óf er ooit iets zal gebeuren, maar eerder: wanneer? En: hoe groot is de impact? Het komt erop aan een goede balans te vinden tussen investeren in cyberveiligheid en operationele efficiëntie. Dat evenwicht is niet zo simpel, maar idealiter houdt de weegschaal telkens iets meer rekening met security.”

> We moeten zo nauwkeurig mogelijk weten wat we precies moeten beveiligen.”
>
> Peter-Jan Deltour

PARTNERS

Ook Cebeo, systeemintegratoren en machinebouwers vertolken een belangrijke rol in het verbeteren van het cybersecurityniveau in onze industrie, vindt Peter-Jan. “Cebeo staat vanuit zijn positie heel dicht bij de markt en heeft veel voeling met wat er leeft. Daardoor beschikt het over een breder draagvlak om zaken te detecteren en advies te geven. Integratoren en machinebouwers kunnen eveneens van goudwaarde zijn, zonder het zelf goed te beseffen.

Voor ondernemingen wordt het namelijk cruciaal om hun hele ‘supply chain’ te beveiligen. Weten dat machines zo goed mogelijk voorzien zijn van cybersecurity, biedt gemoedsrust én schept extra vertrouwen in hun machinebouwers, wat voor die laatsten tot extra mond-tot-mondreclame kan leiden.”

Peter-Jan is lovend over de sensibiliserende inspanningen die het CCB (Center for Cybersecurity Belgium) al langere tijd levert en roept de industrie op om investeren in digitale veiligheid niet tot een dovemanskreet te reduceren. “Zie het niet als een verplichting, maar als een noodzakelijke stap in het veiliger maken van je processen. Als TÜV-gecertificeerde organisatie voor de implementatie van IEC 62443 (zowel qua algemeen management, systeemintegratie als componentbeveiliging), wil Phoenix Contact daar graag toe bijdragen.”

Audi realiseerde met Phoenix Contact, als TÜV-gecertificeerde IEC 62443-2-4-Security Service Provider, al in de planningsfase een 360° beveiligingsconcept.

CEBEO
PARTNERSHIPS
HMS

HMS NODIGT MACHINEBOUWERS UIT OM BEVEILIGINGS-NIVEAUS IN MACHINES TE VERWERKEN

"IEC 62443 is een goede standaard om op verder te bouwen"

Thomas Vasen,
Business Developer Network Security
bij HMS

NIS2: allemaal goed en wel, maar hoe zorg je ervoor dat je conform bent als die richtlijn zich niet echt naar concrete maatregelen vertaalt? Thomas Vasen, Business Developer Network Security bij HMS (Hardware Meets Software), vindt dat België met het CyberFundamentals Framework het goede voorbeeld geeft. "Het toepassen van de IEC 62443-standaard is een handige leidraad voor machinebouwers en de industrie om cybersecurity zo goed mogelijk in de OT-kant van industriële processen te integreren."

Lees verder op pagina 28

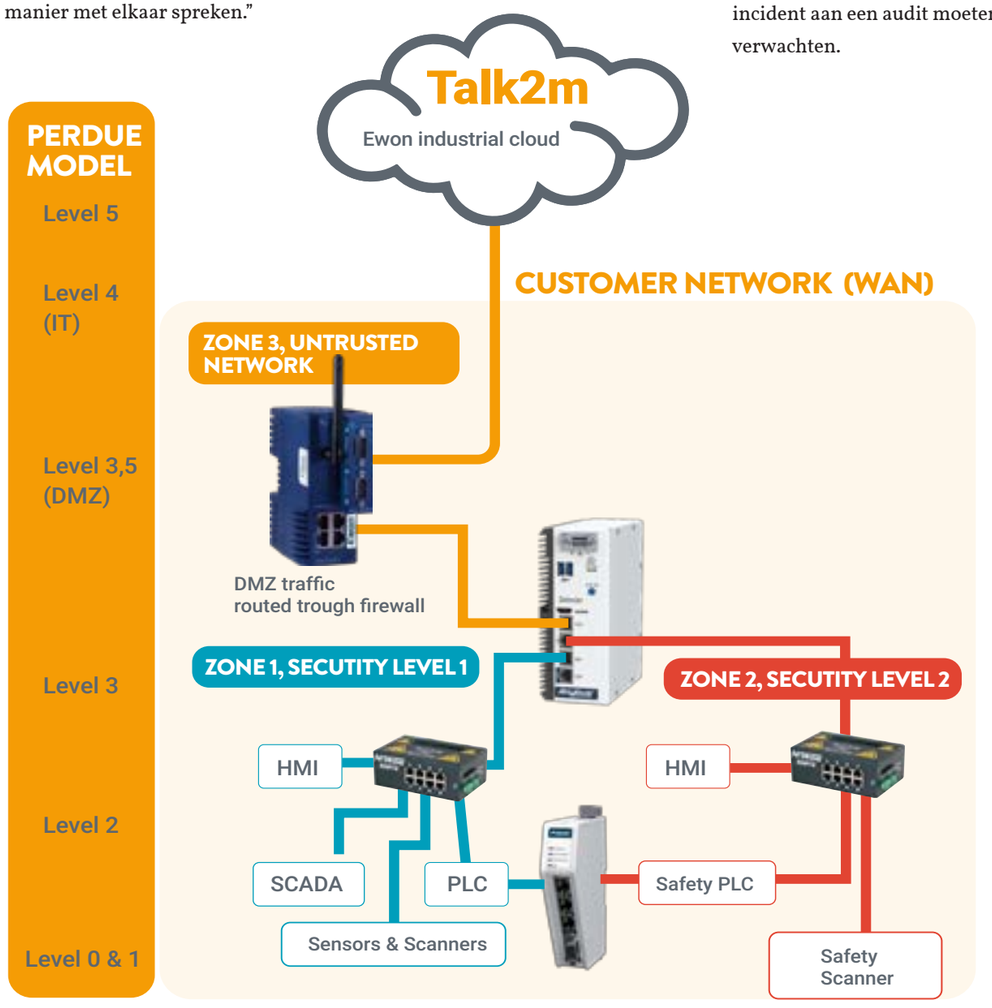
Vervolg van pagina 27

UPGRADE PROTOCOLLEN

Cybersecurity is al vele jaren een essentieel aandachtspunt voor HMS. Daardoor weten ze maar al te goed waar de grootste obstakels zich situeren. “We merken vaak dat er bij het gebruik van industriële protocollen nog geen authenticatie is ingebouwd. Om dat mogelijk te maken, is doorgaans een upgrade van die protocollen nodig, zodat PLC’s (Programmable Logic Controllers) en andere OT-toestellen op een veiligere manier met elkaar spreken.”

Dat is geen evidentie: vaak zijn secure versies nog niet beschikbaar of moeten alle PLC’s en RTU’s (Remote Terminal Units) worden vervangen. Dat gaat gepaard met een heel groot kostenplaatje. Er zijn dus alternatieve strategieën nodig om de OT-netwerken vandaag al te beschermen.

De oplossing is segmentatie, een strategie om machines van elkaar te isoleren en daarmee de communicatie tussen verschillende zones in OT-netwerken te controleren volgens een ‘deny by default’-policy. Alleen: bij implementatie is het vaak nodig de productie tijdelijk stil te leggen en daar knelt natuurlijk het schoentje. “Zeker bedrijven die volgens de NIS2-richtlijnen tot de ‘Andere Kritieke Sectoren’ behoren, voelen minder snel de nood om dat te doen omdat ze zich alleen na een incident aan een audit moeten verwachten.



Bij de ‘NIS2 Zeer Kritieke Sectoren’ ligt dat anders, omdat zij ook onaangekondigd audits kunnen krijgen. Bovendien komt OT-cybersecurity bij heel wat ondernemingen pas op de tweede plaats: de urgentie ligt vooral bij het beveiligen van de IT-kant, ook omdat eventuele storingen aan de OT-zijde vaak hun oorzaak vinden in een IT-probleem.”

STREVEN NAAR DUIDELIJKHEID

Komt daarbij dat in veel Europese landen de NIS2-richtlijn zich niet vertaalt naar concrete nationale wetgeving. “De aanbeveling is om na een risicoanalyse ‘best practices’ te gaan toepassen, maar die zijn voor de meeste sectoren vaak anders. Ergens is het logisch dat Europa zich met NIS2 wat neutraliteit inbouwt op dat vlak, omdat het zich onafhankelijk van certificatiesystemen wil opstellen. Alleen: dat creëert onduidelijkheid. België heeft daar goed op geanticipeerd met de creatie van het CyberFundamentals Framework, een reeks concrete maatregelen die de cyberweerbaarheid van een organisatie moeten vergroten.”

Het CyberFundamentals Framework baseert zich op vier veel gebruikte cyberbeveiligingskaders, waar IEC 62443 er één van is. “Deze reeks normen definieert vereisten en processen voor de implementatie en het onderhoud van elektronisch beveiligde industriële automatiserings- en controlesystemen”, verduidelijkt Thomas. “Wie tussen de regels van NIS2 door kan lezen, begrijpt dat Europa deze standaard als een nuttige leidraad ziet.

Wie IEC 62443 leest, moet zich er misschien even doorworstelen, maar snapt al snel dat de voorgestelde normen daadwerkelijk helpen om naar veiliger industriële processen te evolueren.”

Lees verder op pagina 30

> “OT-cybersecurity komt bij heel wat ondernemingen pas op de tweede plaats.”
>
> Thomas Vasen, Business Developer Network Security bij HMS

Vervolg van pagina 29

HMS helpt industriële eindklanten en machinebouwers om NIS2-conform te worden. “We merken ten eerste een grote behoefte aan training en consultancy. Daar spelen we op in met de Industrial Security Awareness Training, waarin we op een laagdrempelige manier de risico’s uitleggen – onder meer via een demonstratie van een ethische hacker – en eenvoudig verduidelijken hoe je deze uitdaging kan aanpakken.

In een tweede fase kunnen we, samen met systeemintegratoren, een systeem ‘redesignen’: hoe zit een fabriek en het machinepark in elkaar, waar situeren zich de grootste risico’s? Bijvoorbeeld: een yoghurtfabrikant is erbij gebaat om de machine die yoghurt met fruit mengt, zo goed mogelijk te beveiligen. Als daar een probleem optreedt, verlies je veel tijd en geld met het leegmaken en reinigen van de machine.”

BEVEILIGINGSNIVEAUS

Ten derde komt het erop neer het beveiligingsniveau van elke machine te gaan bepalen – idealiter via de 62443-standaard – en daar vervolgens de gewenste eisen voor segmentatie op toe te passen. “Security Level 1 (SL1) vereist alleen een ‘logische’ segmentatie, bij SL 2 is dat ook fysieke segmentatie… Door het machinepark in kleinere segmenten op te delen, verbeter je de beveiliging, de prestaties en de beheerbaarheid. Specifieke beveiligings- en toegangsregels voorkomen dat niet-geautoriseerde gebruikers of bedreigingen zich door het hele netwerk kunnen verspreiden.”

“Wie tussen de regels van NIS2 door kan lezen, begrijpt dat Europa de standaard IEC 62443 als een nuttige leidraad ziet.”

BEWUSTE KEUZE

Thomas nodigt de industrie en machinebouwers uit om NIS2 samen aan te pakken. “Los van alle eisen, is het voorzien van krachtige beveiliging voor je operationele processen vooral een keuze. Kies bewust voor die hogere security en maak gebruik van de 62443-standaard om te evolueren naar een veerkrachtige productieomgeving. Machinebouwers schuiven hun verantwoordelijkheid beter niet af, maar beschouwen NIS2 idealiter als een tool om een nog betere service aan hun klanten te kunnen verzorgen.”

Thomas Vasen ziet hier een belangrijke taak én opportuniteit voor machinebouwers. “Door NIS2 krijgen industriële eindklanten steeds meer vragen van hun verzekeringsmaatschappijen, die willen weten hoe ze hun operationele technologie beveiligen. Dit zal ervoor zorgen dat de industrie aan machinebouwers vraagt om specifieke beveiligingsniveaus in hun machines te integreren. Machinebouwers zouden ervoor kunnen opteren om standaard SL1 te voorzien en vanaf SL2 een hoger prijskaartje te vragen. Dat biedt een win-win-verhaal: de industriële klant is NIS2-conform en voor de machinebouwer is het een verrijking van het businessmodel. Automatisch zou dat tot een hogere netwerkveiligheid leiden.”

CEBEO
IT-AFDELING

"Proactief inspelen
op potentiële dreigingen"

Steven Depuydt, Chief Information Officer bij Cebeo

CEBEO INVESTEERT STERK IN HOOGST MOGELIJKE NIVEAU VAN CYBERSECURITY

Als partner in elektrotechnisch materiaal en oplossingen vindt Cebeo het belangrijk om te tonen hoe je cybersecurity krachtdadig aanpakt. De voorbije jaren is aanzienlijk geïnvesteerd in het versterken en uitbreiden van de IT-afdeling. CIO Steven Depuydt (Chief Information Officer) verduidelijkt hoe onze organisatie van cybersecurity een absolute prioriteit maakt.

Lees verder op pagina 34

Vervolg van pagina 33

Zeven jaar geleden kwam Steven Depuydt bij Cebeo aan boord als eerste voltijdse CIO. “Op dat moment telde de IT-afdeling 24 mensen, vandaag zijn dat er liefst 66. Daarvan zijn twee mensen voltijds bezig met cybersecurity: één persoon doktert de strategie en de planning uit, de andere is actief als security engineer.”

RUN, CHANGE, TRANSFORM

Een eerste aandachtspunt dat Steven introduceerde toen hij begon bij Cebeo, was de planning en uitwerking van de volledige digitale transformatie. “Zowel op het vlak van infrastructuur als op softwarevlak is of wordt alles volledig vernieuwd”, legt hij uit. “Dat weerspiegelt zich onder meer in nieuwe servers, netwerken en een firewall, maar evenzeer in de webshop, systemen voor warehouse- en transportmanagement, enzovoort. De IT-afdeling spitst zich op drie zaken toe: ‘Run’ (alles wat nodig is om optimaal operationeel te zijn), ‘Change’ (veranderingen en geplande innovaties) en ‘Transform’ (alle inspanningen die kaderen in de digitale transformatie). In functie daarvan is een Center of Excellence opgericht, waar ook onze cybersecurity-mensen toe behoren.

Zij werken volgens de ISO27001-standaard (kwaliteitsstandaard voor informatiebeveiliging, red.) en koesteren de ambitie om dat certificaat op termijn te behalen.”

In principe hoeft Cebeo niet aan de NIS2-richtlijn te voldoen, maar desondanks stellen we alles in het werk om een erg hoog niveau van cybersecurity te behalen. “Een recente audit door PWC wees uit dat Cebeo op dat vlak tot de beste landen van de Sonepar-groep, Cebeo’s moederbedrijf, behoort”, gaat Steven verder. “Ook intern gebeuren er regelmatig audits om ons op dat vlak uit te dagen. Zo organiseren we regelmatig phishing- en pen-tests, om te zien in hoeverre onze IT-infrastructuur bestand is tegen potentiële dreigingen. We werken op dat vlak zo proactief mogelijk en zorgen voor sensibilisering en cybertrainingen van onze medewerkers, aangezien het grootste gevaar op ongewenste indringers om de hoek loert als onze medewerkers mogelijk onvoorzichtige IT-handelingen uitvoeren.”

TIEN SLOTGRACHTEN

“Ik hoorde een ethische hacker onlangs vertellen dat je als organisatie niet één, maar tien slotgrachten rond je ‘kasteel’ moet bouwen”, vervolgt Steven. “Daarom doen we ook allerlei inspanningen om onze cybersecurity te optimaliseren. We ervaren het alleszins als een goed signaal van de Sonepar-groep om naar een globale, gecentraliseerde aanpak van dit fenomeen te gaan. De kruisbestuiving tussen de experts uit al die landen zal op dat vlak ongetwijfeld voor een grote toegevoegde waarde zorgen.”

“Als organisatie moet je niet één, maar tien slotgrachten rond je ‘kasteel’ bouwen.”

VARTA Alkaline INDUSTRIAL PRO

VARTA ALKALINE INDUSTRIAL PRO

Is speciaal ontworpen en geproduceerd voor professioneel gebruik. Energie op expertniveau met superieure kwaliteit. Onze premium batterijen zijn de perfecte match als u op zoek bent naar een probleemloze batterijoplossing voor uw apparaten. Sterk geautomatiseerde productieprocessen zorgen voor een uiterst betrouwbaar en veilig product.

- Premiumkwaliteit (Made in Germany)
- Houdbaarheid tot wel 10 jaar*
- Lekvrije technologie
- OEM-vriendelijk productontwerp en verpakking voor eenvoudige handling
- Compleet assortiment dat geschikt is voor tal van professionele toepassingen

*AAA, AA, C, D

VARTA

Make reliable

IMPACT

with PanelSeT enclosures

PanelSeT HD industriële behuizing voor outdoor toepassingen

PanelSeT Heavy Duty behuizingen zijn gemaakt van staal met anti-corrosiecoating.

Life Is On | Schneider Electric

“Meerwaarde bieden via interne en externe kennisdeling”

Florian Delanghe, Product Manager Datacom & Telecom bij Cebeo

SELECTIEGIDS ‘NETWORKS FOR INDUSTRY’

BRUG TUSSEN INDUSTRIE EN DATACOM-OPLOSSINGEN

Connectiviteit speelt een steeds crucialere rol in industriële omgevingen. Als antwoord op de groeiende behoefte breidt Cebeo zijn expertise in datacom voor de tertiaire markt verder uit naar de industriële sector. De nieuwe selectiegids ‘Networks for Industry’, die in 2025 zal uitkomen, biedt daarbij een praktische handleiding én werkdocument.

Vervolg op pagina 40

Vervolg van pagina 39

INDUSTRY MEETS DATACOM

Dataconnectiviteit is een fundamentele vereiste voor de moderne industrie. Sensoren, PLC-sturingen en verbonden apparaten genereren immers real-time data waarmee productieprocessen gedeeld, geanalyseerd en beheerd kunnen worden. Dit leidt tot lagere kosten, hogere productiviteit en minder downtime.

Betrouwbare connectiviteit via koper, glasvezellinks of draadloze verbinding spelen dus een cruciale rol om het productieproces operationeel te houden.

"MEERWAARDE BIEDEN VIA INTERNE EN EXTERNE KENNISDELING"

Florian Delanghe, Product Manager Datacom & Telecom bij Cebeo, benadrukt het belang van de synergie tussen passieve infrastructuur (zoals kabels en connectoren) en actieve componenten (zoals routers en switches): "Tot voor kort waren de twee kennisdomeinen verdeeld over onze afdelingen Cebeo Solutions for Industry en Cebeo Datacom. Omdat de overlap tussen deze twee segmenten steeds belangrijker wordt, zetten we in op kennisdeling. Deze kruisbestuiving stelt ons in staat om sterkere, geïntegreerde datacom-oplossingen aan te bieden voor de industriële markt."

LOGISCH OPGEBOUWDE GIDS

Ter ondersteuning van deze missie lanceert Cebeo in 2025 de selectiegids 'Networks for Industry', een overzichtelijk en veelzijdig naslagwerk. Hiermee slaat het bedrijf de brug tussen datacom-technologie en industriële toepassingen.

Door de gids hoofdzakelijk digitaal aan te bieden, zal ze regelmatig bijgewerkt kunnen worden. Zo blijft het aanbod altijd actueel en relevant. Cebeo is volop bezig met de creatie ervan, maar het zal nog even duren voor de gids beschikbaar is voor klanten.

Industriële klanten die extra ondersteuning nodig hebben, kunnen wel alvast rekenen op advies van de regionale datacom- of industriespecialisten van Cebeo. Op die manier combineert Cebeo zijn uitgebreide expertise met praktische tools.

WAT BIEDT DE GIDS?

- Een breed scala aan oplossingen van betrouwbare leveranciers
- Logische structuur voor snelle en eenvoudige navigatie
- Aandacht voor cybersecurity, inclusief producten die aansluiten bij de nieuwe NIS2-richtlijn

TECHNOLUX

TOEPASSINGEN VOOR ELKE UITDAGING

PAC-D AI

EEN TOESTEL ONTWIKKELD VOOR GEBRUIK IN CORROSIEVE OMGEVINGEN

PAC-D AI is een krachting LEDarmatuur (tot 148 lm/W) ontworpen voor professioneel gebruik in vochtige en stoffige omgevingen en gebieden die blootstaan aan corrosieve dampen zoals ammoniak.
De afdekkap uit opaal metacrylaat (IK03) wordt met onverliesbare inox clipsen bevestigd aan de lichtgrijze basis uit glasvezelversterkt polyester die zorgt voor de waterdichtheid op elke ondergrond. Dankzij de hoge beschermingsgraad IP 69K is het armatuur permanent beschermd tegen het binnendringen van stof en waterstralen wat het uitermate geschikt maakt voor gebruik in stallen, hout - & papierindustrie en opslagruimtes.
Op pagina 255 van de TECHNOLUX 16.0 catalogus kan u een overzicht vinden van de meest voorkomende chemische producten en hun resistentie ten opzicht van de gebruikte materialen.

LZP HT

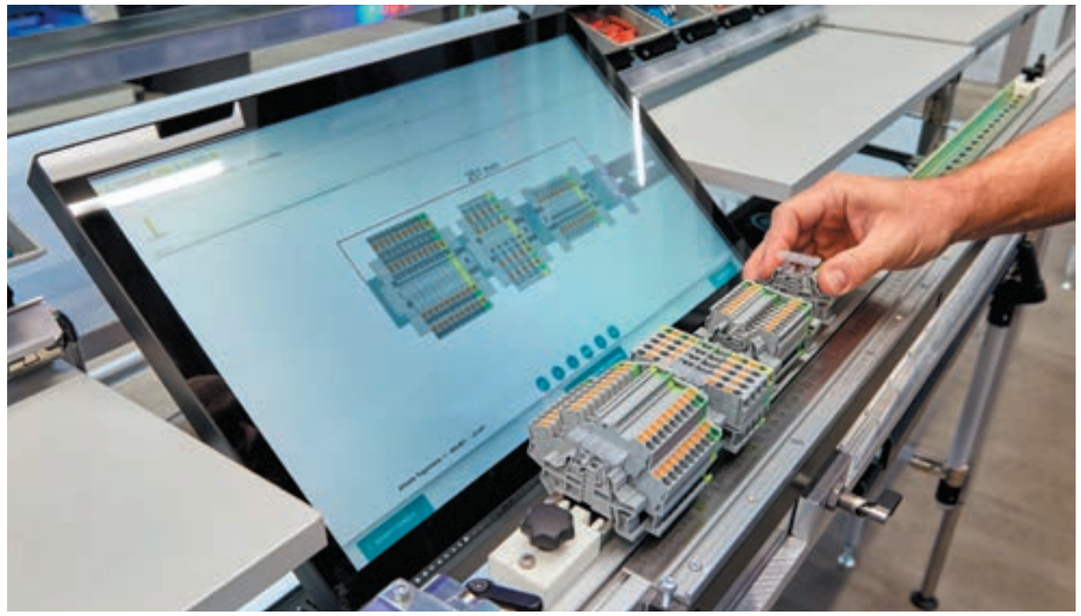
EEN TOESTEL ONTWIKKELD VOOR GEBRUIK IN EEN BREED TEMPERATUUR BEREIK (-40°C TOT +55°C)

Het vochtbestendig LED armatuur LZP HT is een krachtig (tot 132 lm/W) en robuust armatuur voor de industrie. De afdekkap uit opaal polycarbonaat zorgt voor de slagvastheid (IK07) en wordt met onverliesbare inox clipsen bevestigd aan de lichtgrijze basis uit glasvezelversterkt polyester die zorgt voor de waterdichtheid op elke ondergrond.
Met een breed temperatuur bereik van -40°C tot + 55°C kan het armatuur in vele toepassingen ingezet worden.

Beide armaturen worden ontwikkeld en gefabriceerd in Europa en hierbij wordt rekening gehouden met de voorschriften rond duurzaamheid (vervangbare LED modules, recycleerbare materialen, voorschriften rond dierenwelzijn, ...). Door de hoge beschermingsgraden IP 66 en IP 69K kunnen de toestellen onbeschermd buiten geïnstalleerd worden en de HACCP certificatie zorgt er voor dat de types kunnen toegepast worden in de voedingsindustrie.

VRAAG UW TECHNOLUX 16.0 CATALOGUS AAN BIJ UW CONTACTPERSOON OF DOWNLOAD UW EXEMPLAAR VIA WWW.CEBEO.BE

PHOENIX CONTACT



PROCESOPTIMALISATIE TUSSEN UW ONTWERPAFDELING EN DE PRODUCTIE

Speelt de digitalisering van processen en een efficiënte productie een prominente rol in uw bedrijf? Dan bent u bij Phoenix Contact aan het juiste adres. Afhankelijk van uw klantenprofiel hebben we verschillende oplossingen in huis om het productieproces te optimaliseren aan de hand van de beschikbare data uit uw CAE-systeem.

Het efficiënt opbouwen van een DIN-rail met componenten (ook wel een functionele DIN-rail genoemd) is voor ons geen geheim, maar al te vaak zien we bij onze klanten overbodige en handmatige handelingen in het productieproces, wat leidt tot fouten en efficiëntieverlies.

Om onze klanten hierin te ondersteunen, hebben we de software ClipX ENGINEER ontwikkeld.

CLIPX ENGINEER

ClipX ENGINEER is de nieuwe software voor de efficiënte planning van functionele DIN-rails, montageplaten en zelfs schakelkasten! In deze software is een directe koppeling mogelijk met uw CAE-systeem. Alle beschikbare data wordt overgenomen en kan verder worden verrijkt met bijvoorbeeld markeringsmaterialen.

Is uw functionele DIN-rail klaar voor productie? Dan kan alle artikelinformatie naadloos worden doorgegeven aan uw bestelsysteem. Maar het gaat verder: via deze software kunt u direct een bestelling plaatsen bij een van onze VAC-Centers. Zij produceren de complete functionele DIN-rail met alle componenten en markeringen van Phoenix Contact. Na enkele dagen leveren we de functionele DIN-rail kant-en-klaar bij uw bedrijf.

Bent u geen voorstander hiervan of past dit niet in uw bedrijfsproces? Geen probleem! Onze software “ClipX ENGINEER ASSEMBLE” kan u helpen bij het efficiënt opbouwen van uw DIN-rail in eigen huis.

CLIPX ENGINEER ASSEMBLE - ADD-ON – SOFTWARE

De werknemersassistentiesoftware ClipX ENGINEER ASSEMBLE is een geïntegreerde add-on van de engineeringssoftware ClipX ENGINEER. Deze software maakt gebruik van de gegevens uit het engineeringproces om stapsgewijze instructies te genereren voor het opbouwen van functionele DIN-rails. De software is eenvoudig te koppelen met ons Pick-by-Light-systeem.

Bij elke instructie die u moet uitvoeren, zal een LED oplichten met de te gebruiken materialen uit onze klemmentafel, waardoor het zoeken naar componenten verleden tijd is.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Belangrijkste kenmerken:

- Software voor klemmenstrookmontage, inclusief markeren met stapsgewijze instructies
- Webtoepassing die werkt met Edge, Chrome en Firefox
- Directe gegevensovername uit het engineeringproces
- Tijdsbesparing dankzij directe overname van de projectgegevens uit het engineeringproces
- Vereenvoudigde weergave van projecten in de productie met stapsgewijze processtappen
- Fouten vermijden bij het selecteren van de artikelen door de aansturing van een Pick-by-Light-systeem

Kabelsets, patchkabels en kabels
Plug-and-produce in plaats van complexe montage

Kies uit een uitgebreid assortiment voorgemonteerde kabels of neem contact op om individuele signaalkabels voor sensoren of ethernetkabels voor gegevensoverdracht aan te vragen.

Weidmüller

CAMPUS 2025

WIL JE ALS PROFESSIONAL JE TECHNISCHE KENNIS VERDER UITBREIDEN?

Dankzij het Cebeo Campus opleidingsprogramma blijf je ook in 2025 mee met de laatste innovaties in de sector. Eigen Cebeo specialisten of fabrikanten geven praktijkgerichte opleidingen op verschillende kennisniveaus en in diverse domeinen:

HVAC • RENEWABLE ENERGY • HOME & BUILDING AUTOMATION • NETWERKEN • TOEGANGSCONTROLE
VERLICHTING • SECURITY • CONSUMER ELECTRO • INDUSTRIAL AUTOMATION

Neem snel een kijkje en boek nu al je opleiding bij jou in de buurt.
https://www.cebeo.be/nl-be/opleidingen-events

cebeo campus

INDUCTIVE SENSORS THAT MAKE PERFECT SENSE.

THIS IS SICK

Sensor Intelligence.

Kijk eens even om u heen. Iedereen is omringd door vele dingen die ontworpen zijn om ons het leven gemakkelijker te maken. Van zodra men ze gebruikt, vraagt men zich wel eens af hoe men ooit zonder heeft gekund.
Zo gaat het ook met de inductieve sensoren van SICK. Vanaf het moment dat u uw bestelling plaatst, zorgen de sensoren ervoor dat u efficiënter kunt werken. De inductieve sensoren van SICK zijn even duurzaam als betrouwbaar en zorgen ervoor dat u rustig achterover kunt leunen dankzij de snelle levering, de snelle installatie en de vermindering van de onderhouds- en vervangingskosten die u echt zult merken. Eenmaal geïnstalleerd, verhogen ze uw productiviteit, zodat u uw tijd beter kunt gebruiken. Dat vinden wij pas intelligent! www.sick.com/inductive_sensors

SUNGROW × cebeo
A Sonepar Company

Haal meer uit je installatie met Sungrow!

Ontdek onze Utility oplossingen

B680H

De ultieme oplossing voor toegangscontrole

De FAAC B680H is dé slagboom die veelzijdigheid, duurzaamheid en geavanceerde technologie combineert.

Snelheid en precisie
Openings- en sluitingstijd is instelbaar van 1,5 tot 6 seconden

Uitzonderlijk duurzaam
Ontworpen voor intensief gebruik tot meer dan 2 miljoen cycli

Weerbestendig
Bestand tegen extreme weersomstandigheden, IP56 (TÜV)

Hybridetechnologie
Combinatie van hydraulische en borstelloze motoren

Flexibiliteit
Tot 8m met opties voor rechte, knik- of ronde armen

safe zone

green tech

2easy

Of het nu gaat om parkeerterreinen, ondergrondse parkeergarages, industriële locaties of toegangswegen, deze slagboom biedt een betrouwbare en efficiënte oplossing voor elke situatie.

Ontdek hoe de FAAC B680H uw toegangsbeheer naar een hoger niveau tilt.
Bezoek onze website of neem contact op met een van onze experts voor een vrijblijvende offerte of demonstratie. www.faacbenelux.com