‘Maak vakbekwaamheid binnen de veiligheidsketen aantoonbaar’

Cyber security in het industrieel-technisch MKB

Het niveau van de technische automatisering in de grootschalige industrie stijgt snel. Hierdoor kan deze sector kwetsbaar worden voor allerlei vormen van digitale criminaliteit. Hetzelfde geldt voor vitale infrastructuren als de energiedistributie, of geautomatiseerde bruggen, sluizen, gemalen en waterkeringen. Het is inmiddels een veelgehoorde uitspraak: ‘Leg deze cruciale voorzieningen met hun hoog geautomatiseerde technieken ongeoorloofd digitaal stil, en het hele land gaat plat’.

Om dat te voorkomen moeten zij voldoen aan steeds strengere nationale en internationale voorschriften op het gebied van cyber security. Niet alleen organisatorisch en administratief. Ook als het gaat om de automatisering van de primaire technische bedrijfsprocessen.

Aantoonbaar vakbekwaam

Om daaraan te kunnen voldoen stellen zij ook steeds hogere eisen aan hun toeleveranciers en dienstverleners in het industrieel-technische midden- en kleinbedrijf (MKB). Tot deze omvangrijke en belangrijke categorie binnen de Nederlandse economie behoren onder meer machine- en apparatenbouwers, automatiserings- en installatiebedrijven, adviseurs, installateurs en inspecteurs.

In het hoog-geautomatiseerde industriële grootbedrijf neemt het cyber security-bewustzijn snel toe.

Al deze partijen moeten zowel onderling als naar opdrachtgevers toe hun vakbekwaamheid bij de industrieel-technische cyber security steeds nadrukkelijker kunnen aantonen.

Alleen zo kan de digitale veiligheid binnen de keten van industrieel toeleveren en uitbesteden (T&U) als geheel worden opgebouwd, gesloten en gewaarborgd, om te voldoen aan de internationale wet- en regelgeving en de bijbehorende normen.

‘Elevator Pitch’

Het Industrieel Platform Cyber Security bij NEN wil de complexe wet- en regelgeving die hierop van toepassing is ook voor het Nederlandse industrieel-technische MKB toegankelijk houden. Het heeft daartoe een korte en bondige ‘Elevator Pitch’ opgesteld, voor het management in de genoemde en aanverwante sectoren.

Dit document gaat niet over de inhoud van de technische cyber security-norm zelf. Wel maakt het in een paar woorden duidelijk wat het nut en de noodzaak van deze norm is. Aan de hand daarvan kunnen managers binnen het

Ook het industriële MKB raakt steeds hoger geautomatiseerd en digitaal verbonden met haar belangrijkste opdrachtgevers.

industriële en technische MKB in ons land op de eerste plaats bepalen, wie van hun medewerkers deze normen wél inhoudelijk zouden moeten kennen en toepassen.

Training en certificaat

Deze technici kunnen vervolgens bij NEN een 3-daagse training over de internationale cyber security-norm IEC 62443 volgen. Dat is de internationale standaard voor de cyber security van industriële automatisering en controle-systemen.

'Ook steeds hogere eisen voor het industrieel MKB'

De norm biedt praktische handvatten voor het opzetten van een effectief cyber security-beleid voor industriële proces- en productie-omgevingen. Mens, techniek en organisatie sluiten hierbij op elkaar aan. Zowel eindgebruikers en opdrachtgevers als technische dienstverleners hebben hiermee een gezamenlijk en uniform uitgangspunt bij het beschermen van hun primaire technische bedrijfsprocessen tegen cyber-aanvallen.

IACS

De training gaat niet over de technisch-inhoudelijke kennis van de 'Industrial Automation & Control Systems' (IACS). Die mag bij industriële en infrastructurele automatiseerders als bekend worden verondersteld. De training is vooral gericht op de inhoud van het normenkader, dat een gesloten samenwerking van de afzonderlijke disciplines binnen de industriële en infrastructurele veiligheidsketen als geheel mogelijk maakt.
Hierbij gaat het vooral om het beheer, het management en de organisatie rondom de IACS in relatie tot de cyber security.

Bovendien biedt de training ook het MKB handvatten om hun eigen interne geautomatiseerde industriële productie-processen beter te beveiligen. Die worden namelijk in toenemende mate gekoppeld aan de systemen van opdrachtgevers en afnemers.
Op deze wijze kan de digitale industrieel-technische veiligheidsketen als geheel worden gesloten.

Waarborg

Sinds eind 2017 is er bij ieder kwartaal de mogelijkheid om ▶

Europese Wet- en Regelgeving

Nederland heeft een begin gemaakt met het aantoonbaar maken van de vakbekwaamheid van installatietechnisch personeel binnen het vakgebied industriële en infrastructurele cyber security. Lees meer daarover in bijgaand artikel. Hiermee kan onder meer invulling worden gegeven aan de Europese regelgeving die acties bij cyber-incidenten voorschrijft.

NIS/NIB

Op de eerste plaats is er de Europese Richtlijn Network & Information Security (NIS). Of in het Nederlands: Netwerk en informatiebeveiliging (NIB). In het kader van deze richtlijn wordt door de individuele EU-lidstaten zelf bepaald in welke essentiële sectoren cyber-aanvallen verplicht gemeld dienen te worden.
In ons land is het Nederlands Cyber Security Center (NCSC) van het Ministerie van Justitie en Veiligheid het meldpunt voor bedrijven en organisaties in de vitale infrastructuur.

Voor telecommunicatie, de energie- en drinkwatervoorziening, het betalingsverkeer, en luchthavens lijkt dit duidelijk te zijn. Vanuit de EU worden ze omschreven als 'Operators of Essential Services'.
In Nederland is dit 'de vitale infrastructuur'.
Hierdoor hebben ook de beheerders van onder meer sluizen en gemalen, de risicovolle takken van industrie, en onder meer de water- en energievoorziening in ons land een zorgplicht voor voldoende cyber security, ook van de toegepaste technische installaties. Het toezicht daarop is in handen van de het Agentschap Telecom.
De cyber security-normen die hierop van toepassing zijn helpen bij het voldoen aan de primaire eisen in de NIB Richtlijn.

AVG

Daarnaast werd kortgeleden de Europese General Data Protection Regulation (GDPR) in Nederland definitief van kracht als de Algemene Verordening Gegevensbescherming (AVG). Dat is geen Richtlijn, maar een Verordening. Die geldt buiten de nationale wetgeving om direct in alle EU-lidstaten. Met de AVG is de bescherming van persoonsgegevens in alle landen van de EU op dezelfde manier geregeld en gelden in elke lidstaat dezelfde regels.
De AVG zorgt onder meer voor de versterking en uitbreiding van privacy-rechten, meer verantwoordelijkheden voor organisaties en dezelfde, stevige bevoegdheden voor alle Europese privacy-toezichthouders. Eén daarvan is de mogelijkheid om boetes tot 20 miljoen euro op te leggen.

- na de training het examen voor het certificaat af te leggen, ook voor hen die de training al eerder hebben gevolgd. Hiermee kunnen zij hun vakbekwaamheid met betrekking tot de norm IEC 62443 voor deze technische veiligheid waarborgen naar eigen collega's, naar andere technici of bedrijven met wie wordt samengewerkt. En tot slot samen naar hun gezamenlijke opdrachtgevers toe.
  Wie zakt voor het examen kan drie maanden later weer een nieuwe poging doen.
  De training en het examen zijn allebei conform de norm IEC 62443 en sluiten aan bij de bestaande en nieuwe Europese wet- en regelgeving (zie kader).

'Industriële engineers en installateurs zijn onderdeel T&U-keten'

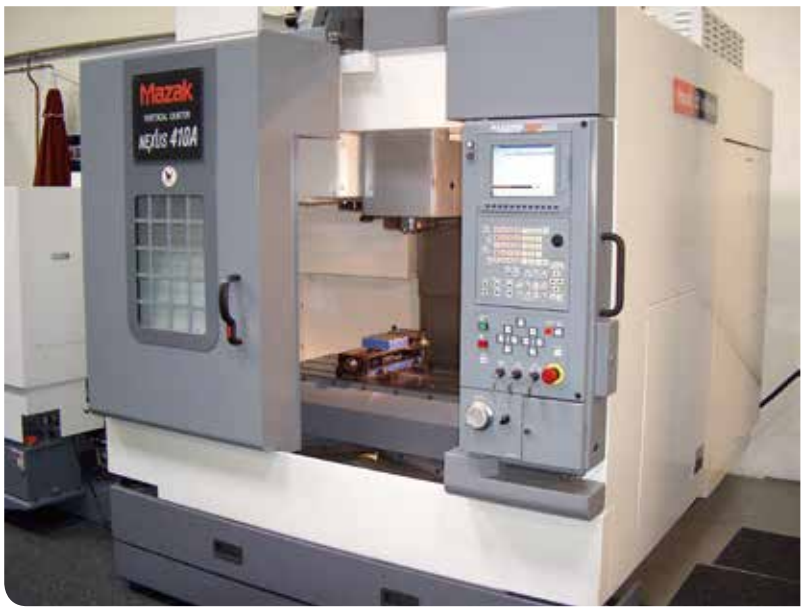
Platform

Het Industrieel Platform Cyber Security bij NEN ondersteunt en bewaakt de onderlinge samenhang en doorontwikkeling van deze en vele andere technische, organisatorische en administratieve normen.
Dit versterkt de positie van Nederlandse industriële en technische MKB-bedrijven bij eventuele juridische geschillen na ongeoorloofde digitale in- en aanvallen bij hun binnen- en buitenlandse opdrachtgevers, met alle mogelijke gevolgen van dien.

Overigens is 1 op de 5 MKB'ers in het verleden zelf ook al eens slachtoffer geworden van cyber crime, vertelt Marcel Jutte, managing director van Hudson Cybertec. Dat is een onafhankelijke cyber security solution provider voor het IACS-domein, ofwel de operationele technologie (OT), in Den Haag.
Jutte: "Tot nu toe is dat meestal nog zonder al te grote gevolgen gebleven. Maar dat kan snel veranderen. Vanwege de aantrekkende economie tegenover een snelgroei-end tekort aan vakbekwaam technisch personeel is het industriële MKB ook haar eigen productieprocessen in toenemende mate aan het automatiseren. Hierbij moeten dezelfde beveiligingsvoorschriften en –normen in acht worden genomen."

Installaties

De producten, installaties, machines en (deel)systemen die het industriële MKB in ons land ontwikkelt en produceert voor het binnen- en buitenlandse grootbedrijf,



zijn tegenwoordig vrijwel allemaal geheel of gedeeltelijk geautomatiseerd. Dat maakt ze snel, flexibel, rendabel, en daardoor ook concurrerend op de internationale markten. Hierdoor worden ze echter steeds kwetsbaarder voor ongeoorloofde inbreuk en misbruik van digitale gegevens, ofwel cyber crime.

'Vakbekwaamheid cyber security nadrukkelijker aantonen'

De speciale wet- en regelgeving die hierop in binnen- en buitenland van toepassing is wordt ook dit jaar weer verder aangescherpt, vertelt Jutte.

Industrieel Platform Cyber Security

Aan het Platform Industrial Cyber Security bij NEN wordt deel genomen door de volgende bedrijven en organisaties:

Alliander
Hudson Cybertec
Dalli de Klok
Gasunie
Honeywell Enraf
EY
Applied Risk
Alewijnse Industrial Automation
Phoenix Contact
Yokogawa
Security Matters
Weidmüller
Rijkswaterstaat
Applied Tech Systems
ENGIE
ICT Automatisering
Viales
Du Pont de Nemours
Hudson Cybertec
Rijkswaterstaat
Akzo Nobel

Voor meer informatie of aanmelding e-mail: elektrische-installaties@nen.nl, of kijk op www.nen.nl/platformcyber-security

Het omvangrijke Nederlandse industriële Midden- en Kleinbedrijf (MKB) is essentieel toeleverancier voor het Europese producerende grootbedrijf. Hierdoor worden ook aan het MKB steeds hogere eisen gesteld op het gebied van cyber security.

Hudson Cybertec is lid van het Industrieel Platform Cyber Security en de hierbij betrokken normcommissies bij de NEN (zie kader). Samen met de NEN verzorgt dit bedrijf de trainingen voor de vakbekwaamheid volgens IEC 62443. De eerste kandidaten van grote industriële installatiebedrijven slaagden eerder dit jaar al voor het examen van de 3-daagse training 'Take control over your security risks with the IEC 62443'.
Met het bijbehorende certificaat kunnen zij nu naar opdrachtgevers toe hun vakbekwaamheid met betrekking tot deze norm aantonen.

Ook MKB

Hudson Cybertec is van oorsprong gericht op cyber security voor industriële automatisering en controlesystemen, zowel in het binnen- als in het buitenland. Zij is actief in met name de grote in het oog springende takken van de risicovolle industrie en de vitale infrastructuur, zoals de energievoorziening , de watersector en de olie- & gas-verwerkende industrie.
Veiligheid en continuïteit van de productieprocessen zijn hierbij al sinds jaar en dag belangrijke aspecten. Door de snelle ontwikkeling en toenemende automatisering en integratie van de IACS-omgevingen, is de noodzaak van cyber security steeds dringender geworden.

In dit segment van de markt is het bewustzijn daarvan de afgelopen jaren snel gestegen, signaleert Jutte. En dat vertaalt zich door naar de eisen die zij stellen aan het enorme aantal industrieel-technische toeleveranciers in het midden- en kleinbedrijf, ook in Nederland. Deze bedrijven dienen nu eveneens aantoonbaar vakbekwaam aan de aangescherpte wet- en regelgeving plus bijbehorende normen voor industriële digitale veiligheid en beveiliging te ▶

De veiligheid van het IoT

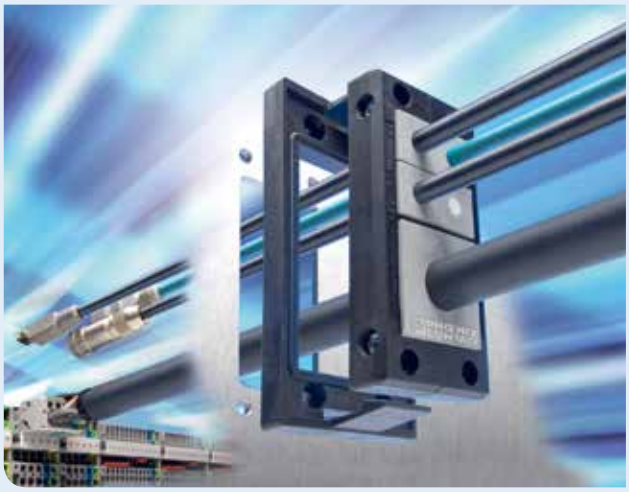
Naast de beveiliging van interne industrieel-technische machines en installaties tegen cyber crime (lees meer daarover in bijgaand artikel) leidt de koppeling hiervan met andere systemen via het openbare Internet of Things (IoT) tot technische uitdagingen bij de beveiliging van informatie en privacy.

De nieuwe Nederlandse werkgroep 'IoT Security en Privacy' bij de NEN staat open voor experts en andere belanghebbenden die namens ons land willen meewerken aan internationale normen hiervoor.

Met het oog op de nieuwe wetgeving op dit gebied, moet al bij het ontwerpen van een industrieel systeem rekening worden gehouden met de beveiliging ervan. Dat gaat het beste door hier afspraken over te maken en deze vast te leggen in normen.
Die worden momenteel ontwikkeld in verschillende gezamenlijke werkgroepen van de Europese en mondiale normalisatie-instituten CEN, CENELEC, ISO en IEC zoals:

- Cyber Security and Data Protection (CEN/CLC/JTC 13)
- Internet of Things and related technologies (ISO/IEC JTC1 SC 41)
- Security Control and Services (ISO/IEC JTC1 SC 27/WG4)

Zij werken aan thema's als productbeveiliging, IoT-betrouwbaarheid, en een richtlijn voor security en privacy op het IoT.



Wie in de Nederlandse werkgroep wil meepraten over deze onderwerpen om zo invloed uit te oefenen op de internationale ontwikkelingen, kan lid worden van de Normcommissie Internet of Things of de Normcommissie Informatiebeveiliging, Cyber Security en Privacy.

Neem voor meer informatie over de werkgroep, deze beide normcommissies of het normalisatieproces, contact op met NEN Kennis- & Informatiediensten via een email naar kid@nen.nl

▶ voldoen. Alleen zo kan uiteindelijk de T&U-keten als geheel worden beveiligd.

De zwakke schakel

Jutte: "Juist in Nederland maken deze MKB-ondernemingen vaak hoogwaardige geautomatiseerde machines, producten en deelsystemen voor de grote, vitale en kwetsbare infrastructuren en takken van industrie in binnen- en buitenland. Dit MKB dreigt nu de zwakke schakel te worden in de cyber security-keten. Deze bedrijven hebben hun interne administratieve en logistieke automatisering doorgaans wel voor elkaar. Net als de industriële automatisering die zij toepassen in hun eigen productielijnen, en in de machines en (deel)systemen die zij toeleveren aan andere sectoren binnen de industrie. Maar dit geldt nog niet voor de aantoonbare beveiliging ervan tegen cyber crime."

IIoT

Dat maakt de industriële en infrastructurele sector als geheel kwetsbaar voor deze vorm van criminaliteit. Zeker nu MKB- en grootbedrijven onder druk van een snel stijgend tekort aan technisch personeel nog directer gaan samenwerken via het Industrial Internet of Things (IIoT). Niet alleen bij de productie, ook daarna bij beheer, onderhoud en inspectie van industriële en infrastructurele systemen en installaties.
Jutte: "Eén zwakke schakel maakt de gehele keten extra kwetsbaar voor cyber crime."

Waterdicht

Met de digitalisering van de samenleving wordt de noodzaak van een waterdicht internationaal systeem voor cyber security dan ook dringender. De Europese Richtlijn Network & Information Security (NIS), in Nederland de Netwerk en Informatiebeveiliging Richtlijn (de NIB-Richtlijn, zie kader) wordt eind dit jaar ook in ons land definitief verplicht via de nationale Cyber Security Wet (CSW).

Sectoren als de ziekenhuizen, of communicatie- en energiebedrijven, en de risicovolle takken binnen de zware industrie hebben dan definitief een meld- en zorgplicht op dit gebied, net als de beheerders van vitale infrastructuren. Daarop wordt toegezien door het Agentschap Telecom. Kijk voor meer informatie hierover op www.agentschaptelecom.nl.

In het kader daarvan dienen bedrijven en organisaties ook eisen te stellen aan hun technische toeleveranciers en dienstverleners binnen het MKB. Diverse overheidsinstanties, eindgebruikers in de vitale infrastructuur, alsmede de eerste industriële installatiebedrijven/systemintegrators hebben hun specialisten op dit gebied al door de NEN laten examineren en certificeren op basis van de norm IEC 62443.

'Alleen zo kan de T&U-keten als geheel worden beveiligd'

Digital Trust Center

Ter ondersteuning van de minder-vitale maar wel kwetsbare sectoren en hun adviseurs binnen het MKB startten eind afgelopen jaar de ministeries van Economische Zaken & Klimaat en Justitie & Veiligheid met de opzet van een 'Digital Trust Centre'. Een van de taken van dit DTC is het bieden van betrouwbare en onafhankelijke informatie aan MKB-bedrijven over digitale kwetsbaarheden, en daarnaast het geven van advies 'hoe te handelen'. Een andere taak van het beoogde DTC is het stimuleren van samenwerkingsverbanden tussen bedrijven op het gebied van cyber security. Kijk voor meer informatie daarover op www.digitaltrustcenter.nl.

De normen

Normen zijn bij dit alles de maatstaven waaraan de afzonderlijke partijen zich samen houden. Cyber crime is grensoverschrijdend. Daarom worden de industrieel-technische CS-normen in internationale verbanden ontwikkeld. Ons land wordt hierbij vertegenwoordigd door Normcommissie NEC 65 voor 'Industrieel meten, regelen en automatiseren'.
Een van de vele tientallen normen die zij ontwikkelen gaat over de cyber security van de installaties en systemen hiervoor. Dat is de IEC 62443 met de titel 'Cyber Security for Industrial Automation and Control Systems'. Deze is binnen de Europese Unie overgenomen en wordt in Nederland binnenkort gepubliceerd als NEN-EN-IEC 62443.
Deze normcommissie wordt bij haar internationale werk ▶

Nieuwe normen en Platform Smart Industry

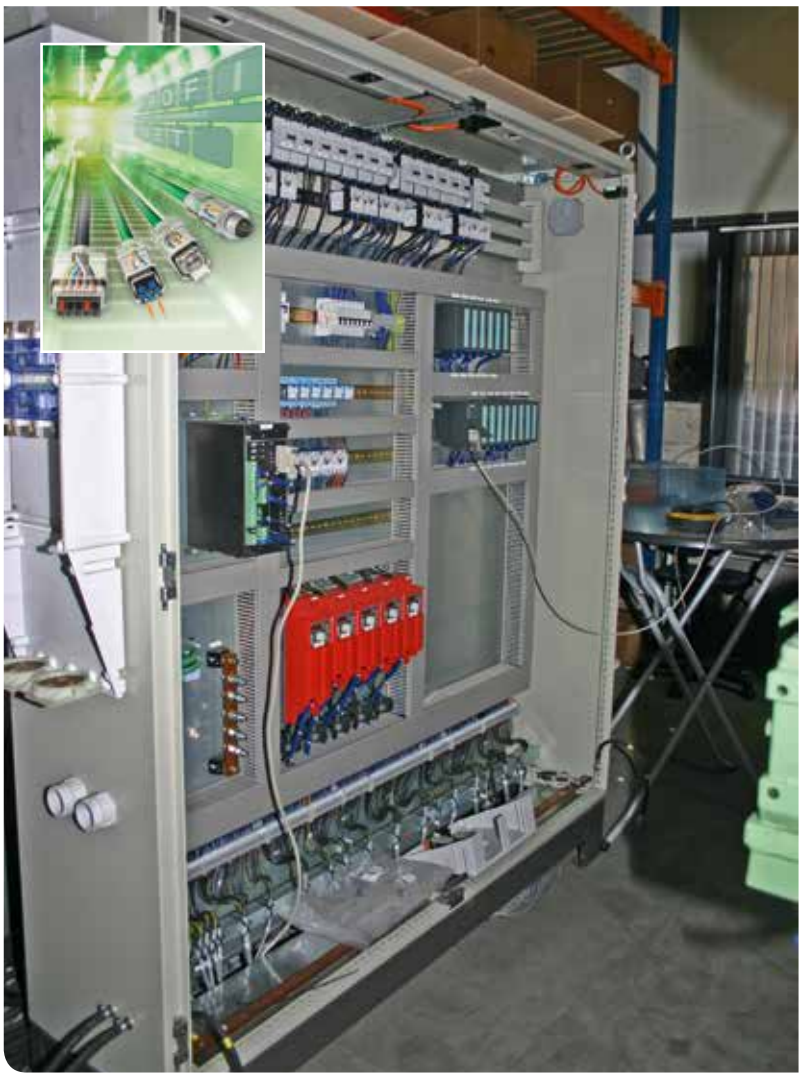
FME, TNO, het ministerie van Economische Zaken en NEN gaan samen met de industrie een Nederlandse agenda opstellen voor de standaardisatie van intelligente netten in de industrie. Want standaardisatie is een belangrijke randvoorwaarde voor de ontwikkeling van een duurzame hoog-rendabele Smart Industry in ons land.

Tijdens het Smart Industry Event eerder dit jaar in Bussum gaven zij samen het startschot voor het Standaardisatieplatform Smart Industry. Dit platform heeft als doelstelling de ontwikkeling en brede toepassing van de normen hiervoor. Daartoe wil zij de betrokkenheid bij de ontwikkeling van die standaarden op Europees en mondiaal niveau aanjagen. Het streven is dat bedrijven meer gebruik maken van de kennis die reeds is vastgelegd in de bestaande normen en dat meer Nederlandse ondernemingen actief gaan meedoen bij de internationale doorontwikkeling hiervan voor de integratie binnen Smart Industry.

Alleen op basis van objectieve en onafhankelijke standaarden, zoals normen, kunnen mensen, machines en automatiseringssystemen in de industrie op een uniforme - en daarmee flexibele - manier aan elkaar worden gekoppeld.
In verschillende projecten wordt gewerkt aan de ontwikkeling van een duurzame en toch rendabele iindustrie. Dat vraagt om een verdergaande mate van automatisering. Zowel bij de 'fieldlabs' hiervoor als bij individuele industriële ondernemingen die hieraan werken leven nog veel vragen.

Bovenstaande vraagstukken worden in Nederland behandeld binnen het nieuwe project Smart Industry Standaardisatie. In nauwe samenwerking met industriële bedrijven hebben FME, TNO, EZ en NEN nu de Nederlandse Standaardisatie Agenda voor Smart Industry opgeleverd. Deze geeft richting aan dit proces en zet aan tot actie.
Lees meer over de industriële normalisatie in ons land in voorgaand artikel.

www.nen.nl/smartindustry



Industriële installateurs maken eveneens deel uit van de T&U-keten, waarvan de digitale veiligheid alleen als geheel kan worden gesloten.

- vanuit de Nederlandse markt ondersteund door verschillende platforms voor gebruikers en toepassers van de normen voor industriële automatisering.
  Het Industrieel Platform Cyber Security heeft onder meer als doel de toepassing van de normen binnen alle schakels van de industriële keten in ons land te stimuleren en mogelijk te maken.

'NEN publiceert een Elevator Pitch voor het technisch MKB'

Europese Technische Commissie

De internationale normen hiervoor sluiten echter nog niet allemaal op elkaar aan, zegt Marcel Jutte als lid van de normcommissie en het platform. Ook die moeten een gesloten keten gaan vormen. Daarom komt er één Europees 'certification framework' voor cyber security, dat wordt ontwikkeld onder toezicht van het European Cyber Security Agency. Certificatieschema's verwijzen naar deze normen.

De Europese normalisatie-instituten CEN en CENELEC vormen één gezamenlijke nieuwe Europese Technische Commissie (TC) voor cyber security en gegevens-bescherming. Deze gaat hiervoor nieuwe technische normen ontwikkelen bij de Europese General Data Protection Regulation (GDPR), die ook in Nederland van kracht is. Daarnaast zijn er organisatorische normen en normen voor informatiebescherming.

Nederlandse commissies

De Nederlandse commissies vertegenwoordigen ons land bij het Europese en mondiale overleg over alle afzonderlijke aspecten. NEC 65 richt zich hierbij op de snel toenemende samenhang van industriële meet- en regelinstrumenten, procesautomatisering, de procesveiligheid en –beveiliging, en dus ook cyber security.
Deze commissie werkt bij NEN samen met andere industriële normcommissies binnen het SIL Platform, het Platform Machineveiligheid, het Platform Analysers en het Industrieel Platform Cyber Security. Lees meer daarover in voorgaand artikel.

MKB-assessment

Hudson Cybertec breidt haar dienstverlening intussen steeds verder uit naar onder meer het industrieel-technisch MKB. Ook het Ministerie van EZK ondersteunt deze schakel in de veiligheidsketen in toenemende mate, samen met de branche- en ondernemersorganisaties binnen MKB-Nederland. Hierbij wordt samengewerkt met universiteiten, kennisinstituten en bedrijven als Hudson Cybertec.
Deze onafhankelijke 'cyber security solution provider' heeft speciale korte 'assessments' en 'scans' ontwikkeld voor ondernemers in het industrieel-technische MKB. Ook deze zijn gebaseerd op de norm IEC 62443.

Industriële installateurs

Jutte: "Vaak hebben deze bedrijven al contact met IT-ers, maar dan gaat het vooral om de administratieve auto-matisering. Nu gaat het om de cyber security van de automatisering in hun eigen productiesystemen, en van de machines en technische systemen die zij leveren aan andere bedrijven. Wanneer zij industriële installateurs, engineers, adviseurs of eigen medewerkers inschakelen die hiervoor zijn opgeleid en gecertificeerd, dan hebben ze al aan een groot deel van hun aangescherpte verplichtingen voldaan."

Stuur voor meer informatie over de normen en de norm-commissie een e-mail naar elektrische-installaties@nen.nl, of kijk op www.nen.nl/platformcybersecurity