auteur Harrie Heemskerk

Nieuwe 3-daagse training van NEN en Hudson Cybertec:

IEC 62443-specialist industriële cyber security

Door de hoge mate van automatisering is de omvang van het digitale dataverkeer in de industrie en infrastructuur de afgelopen jaren sterk toegenomen. Dat maakt ook deze sector steeds gevoeliger voor cyber crime. Vooral in de risicovolle takken van industrie en de kritische infrastructuur kan dat leiden tot zowel economische als maatschappelijke ontwrichting. De energie- en voedselvoorziening, de gezondheidszorg, het milieu en zelfs de nationale veiligheid kunnen hierdoor in gevaar komen. Daarom stellen de Nederlandse en Europese overheid steeds hogere eisen op het gebied van cyber security aan de technische installaties en systemen in deze zogenoemde 'vitale sectoren'.

Hierbij wordt onderscheid gemaakt tussen de technische, administratieve en organisatorische beveiliging van data-beheer, -transmissie en –opslag. Daarop zijn reeds tientallen normen van toepassing, andere zijn nog in ontwikkeling. Basis voor de specifieke technische beveiliging van industriële en infrastructurele ICT-systemen en datanetwerken is de vele delen tellende norm IEC 62443.

De hoge mate van automatisering in de industrie en infrastructuur maakt ook deze sector steeds gevoeliger voor cyber crime.

3-daagse training

Bij deze normreeks heeft NEN samen met de specialisten van Hudson Cybertec in Den Haag een nieuwe 3-daagse training ontwikkeld. Daarin kunnen enerzijds eindgebruikers en operators, en anderzijds system integrators zich laden opleiden tot IEC 62443-specialist industriële cyber security. De training kent daartoe twee afzonderlijke richtingen plus een deel dat ze gezamenlijk volgen, vertelt directeur Marcel Jutte van Hudson Cybertec. In de praktijk werken beide partijen immers ook met elkaar samen.

Verder legt hij uit dat de training niet alleen gericht is op de technisch/inhoudelijke aspecten van de beveiliging van industriële datastromen en opslagsystemen. Daarvoor zorgen de ontwikkelaars en producenten van de beveiligingscomponenten en -systemen (lees meer daarover in het volgende artikel). Bij deze training gaat het meer om de organisatie en het beheer van de technische cyber security.

Platform Industrial Cyber Security

Hudson Cybertec is samen met andere bedrijven en organisaties lid van het Platform Industrial Cyber Security bij NEN. Dat ondersteunt de onderlinge samenhang van de vele andere technische, organisatorische en administratieve normen op het gebied van cyber security, die in verschillen-

De opkomst van het Industrial Internet of Things (IIoT) is niet meer te stuiten. Niet alleen via de bekabeling, maar ook draadloos. Dat maakt industriële systemen nog kwetsbaarder.

de specifieke normcommissies daarvoor worden ontwikkeld. Ook bij Hudson Cybertec zelf werken de afzonderlijke specialisten in de deelgebieden van het brede begrip cyber security nauw met elkaar samen.

'Voor telecommunicatie, gemalen en sluizen, het betalingsverkeer, ziekenhuizen en luchthavens lijkt het belang van cyber security duidelijk'

Smart industry

De Westerse wereld wil ondanks de snelle opmars van ICT een welvarende en vooral veilige samenleving blijven. Dat vraagt om een sterke economische concurrentiepositie. Tegelijkertijd is er de noodzaak tot verduurzaming. Daarover zijn gezamenlijke milieudoelstellingen vastgelegd in internationale verdragen. Dit alles vraagt onder meer om een snelle ontwikkeling en toepassing van nieuwe intelligente technologieën. Technologen spreken zelfs van een nieuwe industriële revolutie, waarin het woord digitalisering centraal staat.

Enkele tientallen jaren geleden al begon de automatisering in de industrie met de eerste PLC's. De digitale datastromen die hierdoor vervolgens ontstonden bleven destijds nog binnen de muren van fabrieken en bedrijven. Hierdoor was de beveiliging ervan nog te overzien.

De afgelopen jaren werd de weg naar smart industry ingeslagen door de integratie en koppeling van alle systemen die in het verleden zijn ontstaan. En intussen vliegen enorme datastromen via het openbare internet en daaraan gekoppelde datacenters nu de hele wereld over.

In principe kan iedereen daar via de digitale snelweg vrij gemakkelijk bij. Ook mensen en organisaties met minder goede bedoelingen.

IoT en IIoT

De opkomst van het Internet of Things (IoT) en het Industrial IoT (IIoT) lijkt nu ook niet meer te stuiten. Dat werd dit jaar duidelijk tijdens verschillende seminars over dit onderwerp en enkele grote industriële vakevenementen in binnen- en buitenland. Daar werden componenten en systemen gepresenteerd waarmee niet alleen nieuwe, maar ook bestaande machines en productielijnen digitaal met elkaar kunnen worden verbonden. Niet alleen via bekabeling, maar ook draadloos. ▶

‘Industrieel meten, regelen en automatiseren’

De Nederlandse normcommissie NEC 65 met de titel ‘Industrieel meten, regelen en automatiseren’ besteedt veel aandacht aan de snel toenemende samenhang van industriële meet- en regelinstrumenten, procesautomatisering, de procesveiligheid en –beveiliging, en het integrale beheer van complete productie-eenheden.

De commissie werkt daartoe bij NEN samen met andere gespecialiseerde normcommissies binnen zogeheten horizontale overlegplatforms voor onder meer SIL, Machineveiligheid, Cyber Security en Analysers. Uniformiteit in de toegepaste besturings-, veiligheids-, ICT- en databeheersystemen op basis van objectieve maatstaven is immers steeds meer noodzaak: het is kostenbesparend en draagt bij aan het optimaal, veilig en duurzaam opereren van integrale productieprocessen.

Normen

Die maatstaven zijn normen. Daaraan kunnen producten, installaties, mensen en processen worden getoetst, op zowel nationaal als internationaal niveau.
NEC 65 zorgt voor de Nederlandse inbreng in de mondiale en Europese normalisatiewerkzaamheden van respectievelijk IEC (TC 65) en Cenelec (TC 65 CX) op het gebied van industrieel meten, regelen en automatiseren. Deze internationale commissies ontwikkelen tevens normen voor de toepassing van veldbussen en bijbehorende protocollen in de industriële meet- en regeltechniek.
TC staat voor Technische Commissie. Onder TC 65 is een groot aantal gespecialiseerde ‘working groups’ (WG’s) actief op tal van specifieke industriële deelgebieden, waaronder de PL- en SIL-normen en die voor industriële cyber security. Lees meer over dit laatste in bijgaand artikel.

Normcommissie NEC 65 bestaat uit de volgende leden:

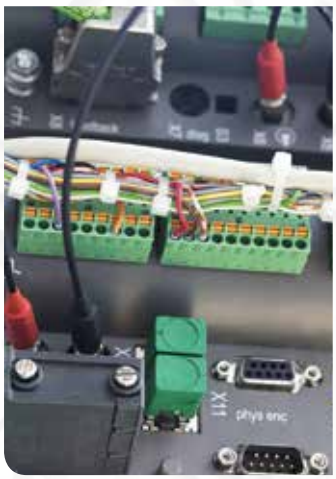
W. van der Bijl, WIB	voorzitter
A.L.M. van Adrichem	Exxon Mobil
E. van Aken	Netbeheer Nederland
A.C.M. Hamers	Honeywell
H. Koning	DSM Nederland
A. de Jong	WIB
R. Lachmann	Emerson
E. Mauro	Yokogawa
A. Meijer	Hudson Cybertec
A.R. Pruijsen	Emerson
F. van Raay	Bosch Rexroth
S. Rutten	Dekra
J.N.H.A.M. School	Honeywell
A. Slagt	Yokogawa

C. Teeuw	Shell
E. van der Wal	PLC-open
R. Wolters	Mokveld
R. Boek-Kroeze	NEN, secretaris

Het Platform Industrial Cyber Security bij deze commissie bestaat uit de volgende leden:

E. van Aken	Alliander, voorzitter
J. Assies	Dalli de Klok
S. Bakker	Gasunie
F. van Bekkum	Honeywell Enraf
A. de Bos	EY
J. Bouhdada	Applied Risk
V.T.J. Gijsen	Alewijnse Industrial Automation
S. Hakstege – Van Eekhout	Phoenix Contact.
M. Hellinghuizer	Yokogawa
R.A. Hulsebos	Enode Industrial Networks
M.H.M. Jutte	Hudson Cybertec
J. van Leeuwen	Weidmüller
M. van Leeuwen	Rijkswaterstaat
B. van der Linden	Applied Tech Systems
A. Meijer	Hudson Cybertec
R. Perrier	Cofely Energy & Infra
P. Roodzant	Cofely Energy & Infra
S. Rutten	Dekra Certification
G.J. Souljé	Du Pont de Nemours
T. Yildirim	Rijkswaterstaat
A. Zwikker	Akzo Nobel N.V.
Mw. R. Boek-Kroeze	NEN, secretaris

Voor meer informatie of aanmelding e-mail de secretaris: elektrische-installaties@nen.nl



Vooral in de risicovolle takken van industrie en de kritische infrastructuur kan cyber crime leiden tot zowel economische als maatschappelijke ontwrichting.

- Via dit IIoT, alle daaraan gekoppelde ICT, en het reguliere internet gaan fabrieken, bedrijven en andere organisaties nog directer en efficiënter met elkaar samenwerken dan ze nu al doen.

'Dus vereist ook de elektriciteitsvoorziening een afdoende niveau van cyber security'

Smart world

Deze ontwikkeling naar smart industry is onderdeel van de digitale revolutie naar een smart world, met duurzame smart houses en smart buildings. Al deze voorzieningen worden door digitale snelwegen met elkaar verbonden en door openbare smart grids voorzien van duurzame energie uit hernieuwbare bronnen. Bij de normalisatie daarvan wordt ons land vertegenwoordigd door weer andere normcommissies en –platforms bij NEN.

Kwetsbaar

Europa wil hierbij voorop blijven lopen en stimuleert deze ontwikkelingen. Net als in ons land onder meer het Ministerie van Economische Zaken en daaraan gelieerde organisaties.

Tegelijkertijd echter blijken al die snel groeiende openbare datastromen, datacenters en andere vormen van dataopslag en –bewerking nieuwe risico's met zich mee te brengen. Dat maakt de slimme samenleving kwetsbaar. Door ongeoorloofd ingrijpen van onbevoegden in datastromen en –opslagsystemen kunnen essentiële processen en voorzieningen in onze samenleving ernstig verstoord raken, of zelfs helemaal worden platgelegd. Bovendien kan hierdoor kostbare informatie worden misbruikt, waarbij ook nog eens de privacy van mensen ernstig in het geding kan raken.

Alle denkbare vormen van deze cyber crime vragen om een voldoende niveau van cyber security. Dat is niet alleen een taak van het bedrijfsleven en de samenleving als geheel, maar ook van de overheid.

De markt

De markt moet er echter eerst zelf de normen voor ont-

De Nederlandse en Europese overheid stellen steeds hogere eisen op het gebied van cyber security aan de technische installaties en systemen in deze zogenoemde 'vitale sectoren'.

NEN heeft samen met de specialisten van Hudson Cybertec in Den Haag een nieuwe 3-daagse training ontwikkeld die enerzijds eindgebruikers en operators, en anderzijds system integrators opleidt tot 'IEC 62443-specialist industriële cyber security'.

wikkelen. Dat zijn de meest objectieve en onafhankelijke maatstaven waaraan producten, installaties, mensen en processen kunnen worden getoetst, op zowel nationaal als internationaal niveau.
Bij de internationale ontwikkeling van de normen specifiek voor industriële cyber security wordt Nederland vertegenwoordigd door Normcommissie NEC 65 bij NEN (zie kader). Andere commissies ontwikkelen de meer administratieve en organisatorische normen voor cyber security.
Maar alleen de overheid kan er bij wet- en regelgeving voor zorgen dat iedereen die bij digitale veiligheid en beveiliging betrokken is, de normen ook daadwerkelijk toepast en handhaaft. Dit overheidstoezicht staat weliswaar nog in de kinderschoenen, maar krijgt nu binnen Europa toch steeds meer vorm. Hierbij zijn ook dit jaar enkele belangrijke stappen gezet.

'IEC 62443 is wereldwijd de standaard voor technisch-industriële cyber security'

Meldplicht Cyber Crime

Allereerst is er de Europese Richtlijn Network & Information Security (NIS), 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 Veiligheid en Justitie hiervoor het meldpunt.
Welke sectoren hier precies onder die richtlijn vallen is nog niet helemaal bekend.

Marcel Jutte: "Voor telecommunicatie, de energie- en drinkwatervoorziening, het betalingsverkeer, en luchthavens lijkt dit duidelijk te zijn. Vanuit de EU wordt gesproken over 'Operators of Essential Services'. De lidstaten bepalen zelf welke organisaties hier onder vallen. Uiteraard zullen dit ook de bedrijven en organisaties zijn die nu al binnen de vitale sector vallen."

Gegevensbescherming

Om de veiligheid en privacy van persoonlijke gegevens in het domein van de administratieve automatisering te waarborgen, werd vervolgens halverwege dit jaar de Europese Algemene Verordening Gegevensbescherming (AVG) van kracht. Dat is geen Richtlijn, maar een Verordening. Die is buiten de nationale wetgeving om direct in alle EU-lidstaten van kracht. In het kader daarvan moeten ook in ons land de organisatorische en administratieve normen op dit gebied daadwerkelijk worden nageleefd. En dat moet indien nodig aantoonbaar worden gemaakt.
Het afgelopen najaar hield de Nederlandse Normcommissie Informatiebeveiliging, Cyber security en Privacy bij NEN hierover een openbare informatiebijeenkomst in het kader van de Europese maand van de Cyber Security.

Vitale infrastructuur

Jutte: "In het kader van de NIB Richtlijn (zie www.nctv.nl) hebben ook de beheerders van vitale infrastructuur als sluizen en gemalen, de risicovolle takken van industrie, en onder meer de water- en energievoorziening in ons land een zorgplicht voor voldoende cyber security. De internationale ontwikkelaars en producenten van de geautomatiseerde besturings- beveiligingssystemen werken al sinds jaar en

dag aan de (door)ontwikkeling van enorme hoeveelheden internationale normen daarvoor."

Platform Industrial Cyber Security

Nederland wordt daarbij vertegenwoordigd door norm-commissie NEC 65 met de titel 'Industrieel meten, regelen en automatiseren'. Deze wordt vanuit het hele land ondersteund door brede gebruikersplatforms van onder meer de zogeheten PL- en SIL-normen voor geautomatiseerde industriële veiligheids- en beveiligingssystemen.

'Dat weten slimme cyber criminelen ook'

Omdat al die systemen in snel toenemende mate ook buiten de eigen fabrieks- en bedrijfsgrenzen communiceren, vragen deze specifieke normen om overkoepelende normen voor cyber security.

De specifieke werkgroepen daarvoor binnen NEC 65 worden ondersteund door het Platform Industrial Cyber Security. De activiteiten van deze normcommissie en platforms strekken zich uit over geautomatiseerde installaties in zowel de industrie als de zogenoemde vitale infrastructuren.

IEC 62443

"Vooral in de meest risicovolle industriële en infrastructurele sectoren zijn de automatiseerders en hun opdrachtgevers zich al jaren bewust van cyber crime en andere veiligheids-risico's", aldus Marcel Jutte. Gezamenlijk ontwikkelden zij al een groot aantal standaarden voor de technische beveiliging ertegen.
De norm IEC 62443 is inmiddels uitgegroeid tot de meest toegepaste wereldwijde standaard voor de beveiliging van de Industrial Automation & Control Systems (IACS) in het Operational Technology (OT) domein. De standaard is ooit opgezet door de International Society of Automation en wordt nu verder door ontwikkeld door het internationale elektro-technische normalisatie-instituut IEC, waarin ook Nederland (NEC) en Europa (Cenelec) zijn vertegenwoordigd.
IEC 62443 biedt oplossingen voor de digitale beveiliging en veiligheid van de primaire processen in industriële organisaties.

Jutte: " Implementatie van deze standaard brengt bedrijven op een hoger niveau van cyber security bonnen het OT-domein, de proces- of productieomgeving binnen de industrie. IEC 62443 is afgeleid van de ISO/IEC 27000-serie. Die is volledig aangepast met de focus op IACS." ▶

Juist de openbare elektriciteitsvoorziening dient gevrijwaard te blijven van cyber crime. Want bij uitval gaat bijna alles plat, ook allerlei veiligheids- en beveiligingssystemen. De netbeheerders zijn dan ook lid van een groot aantal normcommissies en het Platform Industrial Cyber Security bij NEN.

Hudson Cybertec

Hudson Cybertec heeft als cyber security solution provider een 100-procent focus op cyber security binnen dat IACS-domijn, vertelt hij verder. “Wij zijn als Subject Matter Expert (SME) wereldwijd betrokken bij de meest uiteenlopende cyber security vraagstukken.”

In Nederland doen we het op dat gebied nog niet eens zo slecht, is daarbij de ervaring:
“De overheid in ons land stimuleert de cyber awareness al jaren en krijgt hierbij nu meer ondersteuning vanuit de Europese Unie. Een land kan deze veiligheid niet alleen binnen de eigen grenzen regelen. Dat moeten alle EU-lidstaten samen doen. Dataverkeer is immers grenzeloos. De arbeidsveiligheid bijvoorbeeld is in Nederland en de rest van Europa al jarenlang bij wet- en regelgeving vastgelegd en in normen verankerd. Alleen de digitale veiligheid nog niet. Maar deze wordt, ook voor onder meer de arbeidsveiligheid, steeds essentiëler.”

‘Als een energiecentrale plat gaat zijn de gevolgen veel groter’

Schijnveiligheid

Daarom is er ook in Nederland op dit gebied nog heel veel te doen:
“Binnen de verschillende sectoren in de industriële en infrastructurele techniek zijn er nog grote verschillen. Veel organisaties denken het goed voor elkaar te hebben. Maar vaak zijn de systemen nog lek, doordat niet alle aspecten van het geheel zijn afgedekt. Medewerkers denken van elkaar dat de ander het wel geregeld zal hebben. Hierdoor is er veel schijnveiligheid. Dat weten slimme cyber criminelen ook.”

Als voorbeeld maakt hij onderscheid tussen Operationele IT, ofwel OT, en de administratieve IT. Dat zijn vanuit de historie twee heel verschillende werelden, die vragen om totaal andere methoden van beveiliging. De IT-wereld lijkt op sommige vlakken hiermee al veel verder dan de OT. Dit komt door het belang van onder meer de veiligheid van persoonsgegevens en het betalingsverkeer. Maar binnen de OT ligt de focus voornamelijk op de beschikbaarheid, ofwel uptime van de installatie:
“Als een mailserver binnen een organisatie dienst weigert, dan zijn de gevolgen daarvan vaak nog wel te overzien. Maar als een energiecentrale of de elektriciteitsdistributie plat gaat zijn de gevolgen veel groter.”
Operationele, administratie en logistieke processen raken door de voortgaande automatisering echter steeds verder geïntegreerd tot één complex systeem. Ook hierdoor ontstaan er zwakke plekken in de technische beveiliging van het geheel. En daar komt de organisatorische beveiliging dan nog eens bij.

IEC 62443-specialist

Voor een goed gesloten veiligheidsketen is een nauwe samenwerking en aantoonbare vakbekwaamheid van alle betrokken partijen essentieel. De nieuwe driedaagse training van Hudson Cybertec en NEN is vooral daarop gericht.
Jutte: “De training is gericht op cyber security binnen het domein van Industrial Automation & Control Systems (IACS) en voor iedereen toegankelijk, ongeacht het niveau van voorkennis. Er zijn wel twee varianten: één voor de eindgebruikers van IACS in onder meer proces- en SCADA-omgevingen, en één voor de system integrators. Maar misverstanden en bijbehorende risico’s ontstaan vaak doordat er verwarring is over het gebruikte jargon of terminologie. Door deze partijen samen te brengen in de training ontstaan er altijd zinnige discussies met wederzijds begrip als resultaat.”
Met het oog op hun onderlinge samenwerking en begrip wordt de training daarom afgesloten met een gezamenlijke dag.

De opleiding is niet in de eerste plaats gericht op de beveiligingstechniek binnen de IACS zelf, maar meer op het managen ervan. Hij sluit met interactieve componenten en praktijkoefeningen direct aan bij wat er speelt op dit gebied in de werkomgeving van de deelnemers. Zij worden opgeleid tot ‘IEC 62443-specialisten industriële cyber security’, die deze normreeks kunnen toepassen in hun dagelijkse praktijk.

De keten gesloten

Na het voltooien van de training kunnen deelnemers hun vakbekwaamheid vanaf begin komend jaar door NEN laten toetsen, vertelt Jutte tot slot. Want de training is geheel voorbereid op de EU Richtlijnen en komende nationale wetgeving op het gebied van aantoonbare vakbekwaamheid in cyber security binnen het technische domein:
“We zien nu al een duidelijk trend in de markt dat steeds meer bedrijven van system integrators eisen dat zij hun vakbekwaamheid kunnen aantonen. Want pas dan kan de cyber security-keten binnen een industriële of infrastructurele sector als geheel worden gesloten.”

Voor meer informatie en aanmelding: www.nen.nl/training-cybersecurity