Examen in cybersecurity

NEN en Hudson Cybertec hebben gezamenlijk een op de praktijk gebaseerde cursus opgezet voor de IEC 62443 norm. Een examen formaliseert de opgedane kennis, omdat opdrachtgevers steeds vaker om aantoonbare kennis van deze norm vragen. ▷ Rob Hulsebos

NEN is als vertegenwoordiger van de IEC (International Electrotechnical Commission) in Nederland actief op het gebied van cybersecurity. Niet op het technische gebied, maar wel als mede-ontwikkelaar van de normenreeks IEC 62443, specifiek geschreven voor de industriele cybersecurity. Omdat een norm in de basis natuurlijk maar een dikke stapel papier is, heeft NEN in samenwerking met Hudson Cybertec een training ontwikkeld om de implementatie van de IEC 62443 te kunnen bespoedigen. Sinds september is het zelfs mogelijk om bij NEN een examen af te leggen over de IEC 62443. Door het behalen van dit examen kunnen cursisten hun kennis ook daadwerkelijk aantonen.

Waarom NEN en Hudson Cybertec?

Omdat NEN niet zelf de expertise op het gebied van industriële cybersecurity in huis heeft, werkt zij samen met Hudson Cybertec, een van de weinige specialisten in Nederland binnen dit vakgebied. Ik sprak met Joyce Marijnissen - Productmanager bij NEN, en Marcel Jutte - Managing Director bij Hudson Cybertec.

Marijnissen: 'NEN is het Nederlands Normalisatie-instituut en ondersteunt in Nederland het normalisatieproces, met in dit geval de IEC 62443. NEN en Hudson Cybertec kennen elkaar al lange tijd, doordat Hudson Cybertec al vanaf dag één actief betrokken is in het NEN-platform Industrial Platform Cyber Security IPCS.' Daaraan voegt Jutte nog toe: 'De industriële cybersecuritywereld in Nederland is erg klein. Persoonlijk ben ik ook al heel lang betrokken bij de normontwikkeling van de IEC 62443, vroeger ook wel bekend als ISA99. Daarnaast hebben wij uiteraard veel praktijkervaring met cybersecurity in een industriële omgeving, met name in de vitale infrastructuur.'

Waarom is er een eigen training ontwikkeld?

Het doel van de training is om de normenreeks IEC 62443 van theorie om te zetten naar praktijk. Marcel Jutte: 'Als input hiervoor diende uiteraard onze eigen ervaring met cybersecurity in een industriële omgeving. En verder zijn de ervaringen en behoeften uit de Nederlandse en Europese vitale en andere sectoren in de training opgenomen, vertegenwoordigd door brancheorganisaties, opdrachtgevers, overheid en overheidgerelateerde organisaties en partners van zowel NEN als Hudson Cybertec. Ook besteden we aandacht aan de Europese regelgeving op dit gebied.' Joyce Marijnissen geeft daarnaast aan dat de inhoud van de training ieder kwartaal wordt bijgewerkt: 'Dat is erg belangrijk in dit vakgebied, want er verandert heel veel op technisch en juridisch gebied. Onze cursisten waarderen de actualiteit en de praktische insteek van het programma in hoge mate.'

De driedaagse training gaat vooral praktisch in op het gebruik van de IEC 62443. Denk hierbij aan managementmethodiek, uitvoeren van security assessments voor bestaande of nieuwe installaties, risicoanalysemethodiek en het creëren van draagvlak binnen de eigen organisatie. Al deze onderdelen zijn gebaseerd op praktijkvoorbeelden. Hierbij leren de cursisten hoe zij de normenreeks kunnen toepassen in hun eigen organisatie.
De training bestaat uit twee sporen: één voor eindgebruikers en één voor systeemintegratoren en leveranciers. Beide zijn uiteraard bezig met cybersecurity en de IEC 62443, maar soms op een andere manier. De eerste twee dagen volgen beide groepen hetzelfde programma, maar de derde dag is anders. De eindgebruikers gaan dieper in op risicoanalyse, het inrichten van een organisatie en het Cyber Security Management System - CSMS. De systeemintegratoren en leveranciers gaan dieper in op de delen van de IEC 62443 die specifiek voor hen bedoeld zijn. Daarnaast wordt er op de deze dag aandacht besteed aan wetgeving die relevant is voor de desbetreffende groep.

NEN en Hudson Cybertec hebben er bewust voor gekozen om geen aparte trainingen te geven voor beide doelgroepen. Jutte: 'In de communicatie tussen beide groepen ontstaan in de praktijk zo nu en dan problemen. Een voorbeeld hiervan zijn de "vendor requirements", waarin eindgebruikers vastleggen wat zij op het gebied van cybersecurity verwachten van hun systeemintegratoren en leveranciers. We zien dat er vaak interpretatieverschillen zijn als het gaat om de eisen in een bestek en hoe de systeemintegrator deze leest. Door hierover te discussiëren weten beide groepen wat ze van elkaar kunnen verwachten op dit gebied en kan er van elkaar geleerd worden.'

Wetgeving

NEN en Hudson Cybertec vinden het belangrijk om tijdens de training aandacht te schenken aan relevante wetgeving, iets wat tot op heden niet in andere trainingen gebeurt. Sinds 2016 is de wetgeving rondom cybersecurity aangescherpt. Zo is op 6 juli 2016 de Europese cybersecurity-richtlijn "Netwerk- en Informatiebeveiliging" (de NIB-richtlijn, in het Engels: NIS – The Directive on security of network and information systems) uitgekomen. De Europese lidstaten moeten deze binnen 21 maanden in nationale wetgeving omzetten. Bedrijven die actief zijn in de vitale sectoren hebben dan, naast een meldplicht bij het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Veiligheid & Justitie, ook een zorgplicht. Hierbij dienen zij aan te tonen dat de cybersecurity binnen de organisatie op orde is. Welke sectoren in Nederland onder de regelgeving gaan vallen, is op dit moment nog niet definitief vastgesteld. Gedacht kan worden aan energiebedrijven, watervoorziening, waterschappen, banken, ziekenhuizen, telecommunicatiebedrijven en luchthavens, de zogenaamde "Operators of Essential Services".

Verder is in mei 2016 de Europese Algemene Verordening Gegevensbescherming (AVG) in het leven geroepen. Organisaties hebben tot mei 2018 de tijd om hun bedrijfsprocessen volgens de AVG in te richten. Zoals de titel al aangeeft, gaat het hierbij hoofdzakelijk om betere bescherming van persoonsgegevens. Dit is voor industriële systemen zelf nauwelijks van toepassing, maar wél voor de bedrijven die die systemen beheren. Koppelvlakken zullen liggen op gezamenlijke infrastructuur, datakoppelingen, etc. Een slecht beveiligd industrieel netwerk kan dus ook consequenties krijgen voor de compliance met de AVG. Bedrijven die hier niet aan voldoen kunnen zware boetes opgelegd krijgen.

Het examen

Cursisten kunnen sinds september 2017 bij NEN examen doen en een certificaat halen. Het examen wordt één keer per kwartaal afgenomen bij NEN in Delft. Het examen is er, net als de training, in een variant voor eindgebruikers en een variant voor systeemintegratoren en leveranciers. Als de cursist slaagt, geeft het NEN-certificaat aan dat er voldoende kennis is van cybersecurity in een industriële omgeving en dat de cursist in staat is om een beleid op te zetten in overeenstemming met de IEC 62443 en de nieuwe Europese regelgeving (NIS). Marijnissen: 'Het examen formaliseert de opgedane kennis. Vooral voor systeemintegratoren is dit belangrijk, omdat opdrachtgevers bij aanbestedingen steeds vaker om aantoonbare kennis van de IEC 62443-normenreeks vragen.'

Voor buitenlandse cursisten is het ook mogelijk om het NEN-examen af te leggen, deze is namelijk in het Engels. NEN opereert als internationaal vertegenwoordiger van de IEC. De IEC 62443-normenreeks voldoet aan de eisen van de NIS-richtlijn, waardoor deze in heel Europa toepasbaar is.