IEC 62443 biedt steeds vaker uitkomst om compliant te worden

# Hoe de procesindustrie profiteert van NIS2

Nadat Nederland een aantal jaren geleden al kennis mocht maken met de NIS (Network and Information Security) 'directive' en de daaruit voortvloeiende Wbni (Wet beveiliging netwerk- en informatiesystemen) is het inmiddels tijd voor een opvolger, de NIS2. Over ongeveer een jaar zullen bedrijven en organisaties die NIS2-plichtig worden, moeten voldoen aan de aangescherpte wetgeving die hieruit voortkomt. De nieuwe wetgeving hiervoor is op dit moment in voorbereiding. De internetconsultatie die oorspronkelijk vóór afgelopen zomer zou plaatsvinden lijkt nu voor de tweede keer vertraagd, terwijl de door de Europese Unie gestelde datum, waarop alle lidstaten van de Europese Unie de richtlijn geïmplementeerd moeten hebben in nationale wetgeving, met rasse schreden nadert.

Gelukkig komt de NIS2 voor veel organisaties in de procesindustrie niet als verrassing. Veel organisaties in de betrokken sectoren dienen al te voldoen aan de NIS. De NIS2 vormt voor hen vooral een aanscherping van de wetgeving. De sector neemt cybersecurity net als veiligheid zeer serieus en is vaak al verder dan andere sectoren. Zo zijn sommige organisaties al jaren bezig om niet alleen hun eigen digitale weerbaarheid op orde te houden, maar kijken zij ook naar de cybersecurity-volwassenheid van hun toeleveranciers en de cybersecurity van de producten en oplossingen die zij leveren, daarbij geholpen door Hudson Cybertec en Kiwa. De bedrijven hebben er belang bij dat hun leveranciers producten en diensten leveren die aansluiten bij hun eigen behoeften en hun vaak scherpere veiligheidsbeleid.

De NIS2 gaat in op de ketenverantwoordelijkheid van toeleveranciers en speelt daarmee de procesindustrie in de kaart. Waar bedrijven eerst leveranciers moesten overtuigen van de noodzaak van cybersecurity, worden zij nu in de rug gesteund door de NIS2. Immers, de NIS2 legt ook verantwoordelijkheid neer in de toeleveringsketen en verplicht leveranciers cybersecurity te implementeren binnen hun organisatie, producten en diensten. En ook weer binnen hun eigen keten. Zo neemt de digitale weerbaarheid binnen de hele keten toe en maakt dit ook de procesindustrie zelf weerbaarder.

Bij Hudson Cybertec en Kiwa is te zien dat bedrijven in de procesindustrie, net als toeleveranciers, steeds vaker hun heil zoeken bij de IEC 62443 (het internationale de facto normenkader voor cybersecurity binnen de Operationele Technologie) om compliant te worden aan wet- en regelgeving en om cybersecurity gestructureerd en risicogestuurd te managen. Het normenkader wordt gebruikt voor certificering van productontwikkeling en voor aantoonbaarheid van overeenstemming met technische vereisten volgens de 'security levels' uit de norm. Zo worden niet alleen bedrijven, maar ook de toeleveringsketen binnen de procesindustrie digitaal weerbaarder.

**Michael Theuerzeit • Lead consultant bij Hudson Cybertec • www.hudsoncybertec.com**
**info@hudsoncybertec.com**