Het begint al bij procurement

Cybersecurity borgen in uw organisatie?

Steeds vaker krijgt cybersecurity een prominente rol binnen automatiseringsprojecten. Toch hebben veel bedrijven nog moeite met het vinden van de juiste weg. Dat resulteert dan in projecten die worden uitgevoerd met cyber security als een 'after thought'. Hierdoor zijn er geregeld kostbare wijzigingen nodig in het design van systemen of netwerken. Soms worden deze voor cyber security noodzakelijke wijzigingen niet doorgevoerd omdat de kosten voor de aanpassingen achteraf simpelweg te hoog zijn.

Michael Theuerzeit

Gelukkig zien we ook dat het anders kan. Hudson Cybertec, cyber security solution provider voor de Operationele Technologie, is betrokken bij verschillende Scandinavische projecten in de olie & gas industrie. Eén van deze projecten behelst de risk & vulnerability analyse van de ICT-infrastructuur voor het volledige Johan Sverdrup fieldcenter.
Het Johan Sverdrup olieveld is één van de grootste Noorse olievelden en de grootste offshore olievondst in de Noordzee in 30 jaar. Na volledige ontwikkeling, wordt er verwacht dat het enorme olieveld 550-650 duizend vaten olie per dag kan produceren.
De exploitatie van het veld is één van de belangrijkste industriële projecten in Noorwegen voor de komende 50 jaar. De initiële investering voor de eerste fase wordt geschat op ongeveer € 13,5 miljard.

Bij projecten van deze omvang is cybersecurity natuurlijk volledig doorgedrongen in elke vezel van het project. Cybersecurity wordt binnen het hele proces integraal meegenomen, eigenlijk al vanaf het moment dat er over exploitatie van de ontdekte olie- of gasvelden wordt nagedacht.

Hoe bewaak je de cyber security integriteit van de geleverde goederen gedurende de periode van transport en opslag tot aan het moment dat deze uiteindelijk wordt geplaatst?

Procurement

Dat begint al bij procurement. Door bij de aanbesteding van een opdracht cybersecurity al integraal mee te nemen, wordt het een onderdeel van het volledige proces. Er worden cybersecurity eisen gesteld aan leveranciers en system integrators.
Bij aanbestedingen wordt aantoonbare kennis en ervaring met de IEC 62443 norm vereist, inmiddels de facto cybersecurity norm voor Industrial Automation & Control Systems (IACS). De IEC 62443 geeft handvatten voor elke organisatie, van eindgebruiker tot leverancier, gedurende elke fase van een project. Steeds meer system integrators en leveranciers zijn dan ook druk doende om kennis op te bouwen over deze norm.

FEED

Omdat cybersecurity vanaf het begin wordt meegenomen in het gehele proces, is er tijdens de (pre) FEED-fase (Front-End Engineering Design) al aandacht voor cybersecurity. Hierdoor is er bij het vaststellen van de technische vereisten voor het project al de noodzaak om te onderzoeken hoe cybersecurity ingrijpt op het uiteindelijke design. Hudson Cybertec helpt verschillende EPC contractors met de ontwikkeling van onder andere Cyber Security Design Specification documenten om te borgen dat cybersecurity door alle betrokken leveranciers serieus wordt genomen.

Risico- en kwetsbaarhedenanalyses

Gedurende de Detailed Engineering fase werken de leveranciers samen met de EPC- of EPCI-contractor om cybersecurity te borgen in het uiteindelijke design. Hudson Cybertec werkt hierbij steeds nauw samen met een groot aantal leveranciers om een risico- en kwetsbaarheden analyse uit te voeren op alle relevante aan te leveren packages. Gedurende deze analyse wordt door een team van cybersecurity experts van Hudson Cybertec, over zowel het gehele design als over de individuele packages, onderzocht welke kwetsbaarheden er aanwezig zijn in software en hardware die de leverancier in wil zetten. Op basis van de daaraan verbonden risico's kan het noodzakelijk zijn dat er wijzigingen in configuraties of design worden doorgevoerd. Hierbij worden alle relevante aspecten, van actuators tot frequency drives en van telecomsystemen tot safety integrated systems (SIS) meegenomen.

Continue borging van cybersecurity

Als na het FAT-en van de (deel-)levering alle apparatuur naar de construction yard wordt verscheept, begint de volgende uitdaging. Want hoe bewaak je de cyber security integriteit van de geleverde goederen gedurende de periode van transport en opslag tot aan het moment dat deze uiteindelijk wordt geplaatst? Ook hier werken de cybersecurityspecialisten van Hudson Cybertec nauw samen met de experts van oliebedrijven en EPC-contractors, aan oplossingen om ook hier de integriteit en cybersecurity te borgen.

Commissioning en oplevering

Ook tijdens het afbouwen van platformen, als deze eenmaal op de gewenste locatie liggen en de daaropvolgende commissioning, zijn daar veel verschillende contractors dagelijks aan het werk. Het grote aantal personen dat toegang heeft zorgt hier wederom voor additionele cyber security risico's. Ook deze risico's dienen weer gemanaged te worden.
Bij de oplevering van de platformen hoort ook de overdracht van de verantwoording voor cybersecurity. De exploitant en eigenaar van de platformen wordt vanaf dat moment ook verantwoordelijk voor het managen van cybersecurity. Vanaf de eerste dag tot aan het einde van de life-cycle van het platform, dat zomaar een halve eeuw in de toekomst ligt. Hiervoor liggen strakke scenario's klaar om cybersecurity te borgen gedurende de gehele life-cycle.

Hiervoor liggen strakke scenario's klaar om cybersecurity te borgen gedurende de gehele life-cycle...

Grote voordelen

Gedurende de volledige levensfase van het platform, van de eerste ruwe schets op papier tot aan de afschrijving over tientallen jaren, speelt cybersecurity een significante rol bij het op een veilige manier kunnen produceren van olie. De volwassen manier waarop de olie & gas industrie omgaat met cybersecurity levert uiteindelijk grote voordelen op. Hudson Cybertec speelt in de samenwerking met EPC contractors en oliemaatschappijen een centrale rol op het gebied van cybersecurity.

Leveranciers worden actief betrokken en begeleid bij het cybersecurityproces, waardoor er een lage learning curve is. Zij kunnen zich vervolgens positief onderscheiden in toekomstige projecten, door de eerdere ervaring met cybersecurity. Leveranciers die niet mee willen werken, lopen een serieus risico op een lagere ranking op de short list voor komende projecten. Dit leidt uiteindelijk tot flinke kostenbesparingen en hierdoor sluit cybersecurity optimaal aan bij de behoefte.

Lessons learned

Een van de belangrijkste lessons learned, uit de ervaringen van de olie & gas industrie, is dat het belangrijk is om tijdig met cybersecurity te beginnen. Weet uw organisatie niet waar te starten met cybersecurity? Het is essentieel om tenminste te weten waar uw bedrijf op dit moment staat. Een nulmeting geeft dit inzicht. Hudson Cybertec voert deze nulmetingen met grote regelmaat uit. Door de opdrachtgevers te betrekken bij het proces, nemen zij hun lessons learned weer mee in volgende stappen op het gebied van cybersecurity. Zo bouwen zij zelf actief en succesvol mee aan het kennisniveau binnen hun organisatie.