De gehele plant lifecycle cyber secure met de IEC 62443 standaard

Cyber security voor Industrial Automation & Control Systems die de primaire processen van bedrijven besturen, krijgt steeds meer aandacht in de diverse media. Bedrijven kunnen er niet meer onderuit te erkennen dat ook zij hun primaire processen dienen te beveiligen.

Hoewel de eerste cyber security bewustwording bij veel bedrijven al aanwezig is, worstelt een groot aantal nog met de aanpak daarvan en heeft men geen idee hoe zelfs maar te beginnen met het mitigeren van de security risico's. Het gaat hier immers over risico's die een impact kunnen hebben op de aansturing van processen die plaatsvinden in de fysieke wereld en niet over risico's die verbonden zijn aan bijvoorbeeld het gebruik van email. Laat staan dat men weet hoe cyber security binnen deze omgevingen meetbaar te maken en te managen.

Het begint allemaal met de keuze voor een security standaard die aansluit bij de security behoefte van (de aansturing van) de primaire processen van de organisatie. Soms lijkt het voor de hand te liggen om het informatiebeveiligingsbeleid uit de kantoororganisatie (vaak gestoeld op ISO 27K) door te trekken. Maar het gaat hier om de beveiliging van primaire processen, niet om beveiliging van informatie. Voor het nemen van passende security maatregelen voor de Industrial Automation & Control Systems die deze primaire processen besturen en bewaken, is een passende standaard nodig.

De wereldwijd gebruikte IEC 62443 standaard is speciaal voor dit doel ontwikkeld.

Deze standaard houdt rekening met cyber security gedurende de gehele lifecycle van de plant of technische installatie. Vanaf een eerste oriëntatie met systeem scoping en risico analyses voor het globale ontwerp, worden ook detailed design, FAT, commissioning, operations en maintenance, tot zelfs decommissioning meegenomen en gemanaged binnen de IEC 62443. De standaard kan in elk stadium van de plant lifecycle worden geïmplementeerd en zo een bijdrage leveren aan het verbeteren van de cyber security.

Om bedrijven bekend te maken met deze standaard en kennis op laten doen hoe deze standaard op een juiste wijze in te zetten, biedt het IEC 62443 Competence Center van Hudson Cybertec een volledig trainingsprogramma. Bedrijven die hulp willen met de implementatie van deze standaard kunnen hiervoor terecht bij Hudson Cybertec. Daarbij wordt eerst het huidige security niveau van de Industrial Automation & Control Systems in kaart gebracht en het gewenste security niveau bepaald.

Bedrijven krijgen zo duidelijke en meetbare doelen voor cyber security. Dit helpt hen bij het opstellen van de juiste security eisen aan leveranciers bij aanpassingen of vernieuwingen in de technische infrastructuur. Bij nieuwe projecten kan cyber security vervolgens vanaf eerste begin worden gemanaged gedurende de gehele lifecycle. Hierdoor sluiten nieuwe projecten naadloos aan bij het dan reeds bestaande securitybeleid. Dit brengt de cyber security kosten voor nieuwe projecten omlaag.

De IEC 62443 standaard maakt het voor bedrijven mogelijk om de pijlers van cyber security: mens, organisatie en techniek, op juiste wijze te managen. Hiermee wordt cyber security op een verantwoorde wijze verankerd in de bedrijfsvoering en kunnen security doelstellingen meetbaar worden behaald. Zo wordt het security niveau voor de primaire processen blijvend verbeterd en is de organisatie wat cyber security betreft, klaar voor de toekomst.

Meer informatie:
www.hudsoncybertec.com