Industrie 4.0 – hoe een nieuwe machine van bij het ontwerp beveiligen?

02 juni 2017, 02:00

Véronique Dossogne

De betrouwbare en permanent beveiligde werking van wereldwijd geconnecteerde machines en systemen vrijwaren is een essentiële uitdaging die van bij het ontwerp moet worden aangepakt, wil IIoT (Industrial Internet of Things) / Industrie 4.0 met succes worden geïmplementeerd. Precies daarom heeft VDMA (Verband Deutscher Maschinen- und Anlagenbau) een reeks minimale veiligheidsvereisten voor toekomstige machines en fabrieken uitgewerkt.

Cyberbeveiliging is een belangrijk aspect voor een slimme fabriek van zodra het netwerk via het internet verbonden IT-systemen behelst. Daarnaast is een van de basisideeën van Industrie 4.0 de integratie van toeleveringsketens over locaties en bedrijven heen. Het netwerken van de productie geeft echter aanleiding tot mogelijke doelwitten voor spionage. Het probleem is dat er wel beproefde aanbevelingen en normen voor de klassieke IT-veiligheid bestaan, maar niet voor de privacy van machinegegevens. De richtlijnen die VDMA heeft gepubliceerd, 'Industrie 4.0 Security Guidelines : recommendations for actions', geven machinefabrikanten en integrators enkele elementaire tips mee.

Veiligheid van bij ontwerp

Cyberbeveiliging draait rond de bescherming van IT-systemen. Indien die systemen via de integratie van Industrie 4.0 verbonden zijn, dienen zowel de fabrikanten als de operatoren na te denken over de continue beveiliging van deze connectiviteit over de bedrijven heen. Dit aspect staat centraal bij de veiligheid van Industrie 4.0, die tot doel strekt de veiligheid van toekomstige machines en fabrieken gedurende hun volledige levenscyclus te vrijwaren, veeleer dan de huidige situatie waarbij veiligheidsfuncties later moeten worden behandeld.

De integratie van ‘veiligheid van bij het ontwerp’ betekent dat deze functie uiteindelijk als een component van de toekomstige fabrieken en systemen moet worden beschouwd, waarbij ‘veiligheid als een functie’ wordt ingevoerd. Deze richtlijnen bieden de kans om specifieke aspecten uit te lichten en ze zelf te beoordelen. De focus ligt op het oogpunt van de fabrikanten en integrators.

Aanbevelingen

In dit document worden fundamentele aanbevelingen voor actie en minimale vereisten voor beschermende maatregelen uiteengezet die een basisniveau van bescherming voor de machines mogelijk maken. Iedere aanbeveling is ook aan een overeenkomstige productfunctie gekoppeld,

zodat de relevante beschermingsmaatregelen slechts dienen te worden geïdentificeerd voor de respectieve machine tijdens de ontwikkeling. Dit compromis betekent een enorme toename van de cyberbeveiliging voor bedrijven die Industrie 4.0 nastreven.

De productfuncties zijn ook gekoppeld aan actieaanbevelingen (zie figuur 2), om aan te geven op welk punt een actieaanbeveling een minimale vereiste wordt op de Industrie 4.0-schaal van een tot vijf – met andere woorden vanaf welke functionaliteit een beschermingsmaatregel moet worden ingevoerd. De ‘VDMA Industrie 4.0 Toolbox – Producten’ (zie figuur 1) wordt hiertoe als een schaal gebruikt.



(Bron : Industrie 4.0 Security Guidelines : recommendations for actions
Figuur 1 : VDMA Industrie 4.0 Toolbox – Producten: functieklassen van een machine. Binnen de klassen (A tot F) wordt een Industrie 4.0-functionaliteitsschaal van 1 tot 5 gehanteerd. De waarden in de linkerkolom verwijzen naar een klassieke productiemachine; de rechterkolom geeft de volledige visie van Industrie 4.0 weer.')



(Bron :Industrie 4.0 Security Guidelines : recommendations for actions
Figuur 2 : Voorbeeld van een actieaanbeveling. Deze grafiek toont dat de aanbeveling een minimale vereiste wordt van zodra een product minstens een fieldbus-interface of gegevensopslagsysteem voor informatie-uitwisseling heeft.

Deze richtlijnen stellen 85 aanbevelingen voor die in 17 principes zijn geclassificeerd. De algemene principes die op alle IoT-apparaten (vanuit het oogpunt van de fabrikanten) moeten worden toegepast zijn de volgende:

- Invoering van updatemechanismes (indien nodig)
- Documenteren van de interfaces en datatransmissie
- Gebruik van beveiligde protocols
- Beveiliging van de maintenance op afstand
- Consolidering van componenten en software
- Invoering van authenticatiefuncties
- Gebruik van cryptografie
- Training van de productontwikkelaars in de cyberbeveiliging van bij het ontwerp
- Testen van de cyberbeveiliging van producten en implementaties

De vermelde actieaanbevelingen zijn bedoeld als basisbescherming voor een kleine of middelgrote onderneming die Industrie 4.0 nastreeft. Als de eerste stappen reeds werden ondernomen en de machine voor de toekomst moet worden ontworpen met volledige Industrie 4.0-functionaliteit, loont het de moeite om de aanvullende documentatie door te nemen.

Hieronder vindt u een lijst van belangrijke informatiebronnen die extra hulp kunnen bieden bij de invoering van een veilige bescherming.

In het Engels

- VdS Quick Check Security
- Platform Industrie 4.0 Guidelines IT security in Industrie 4.0 : first steps towards secure production
- Platform Industrie 4.0 Guidelines IT security in Industrie 4.0 : action fields for operator
- BSI ICS Security Compendium
- ICS-CERT newsletter, reports and recommendations for action
- ISO/IEC 27000 series on information security
- IEC 62443 Industrial communication networks - Network and system security
- ISO/IEC 15408-1 Evaluation criteria for IT security
- NAMUR worksheet NE 153
- NAMUR worksheet NE 115

In het Duits

- Light and Right Security ICS (LARS ICS)

Met de steun van de FOD Economie heeft Sirris de Normenantenne Industrie 4.0 opgericht, een dienst die werd ingericht om de Belgische ondernemingen, en in hoofdzaak de kmo's, te informeren over de bestaande en toekomstige normen.

Auteurs



Véronique Dossogne