Vertrouwelijkheid: Intern

Ondersteunend document

Vereisten inzake cyberveiligheid voor leveranciers

Inhoudstafel

0 Referentie

Documentnummer	Titel
NVT	ENGIE Industrial Control System security Framework
ZNO. 10010571878.000	Vereiste IT beveiliging for PCS
NVT – zie WWW	Vereiste beveiliging voor Leveranciers IEC 62443-2-4

1 Inleiding

Industriële controlesystemen (ICS) zijn een ruime notie en bestrijken uiteenlopende types van controlesystemen, zoals onder meer Supervisory Control & Data Acquisition systemen (SCADA), gedistribueerde controlesystemen (DCS) maar ook kleinere controlesystemen zoals op een skid gemonteerde Programmable Logic Controllers (PLC). Dergelijke systemen zijn aanwezig in de industriële netwerken en kritieke infrastructuren van ENGIE.

Deze controlesystemen zijn in die zin kritiek voor de werking van de EBL infrastructuren omdat het meestal om hecht verbonden en onderling afhankelijke systemen gaat.

Dit document wil een geconsolideerd overzicht bieden van beste praktijken die aangewezen zijn voor het uitbouwen en handhaven van veilige industriële controlesystemen (ICS), met inbegrip van Supervisory Control & Data Acquisition systemen (SCADA), gedistribueerde controlesystemen (DCS) en andere systemen die een combinatie van IT- en controlefuncties uitvoeren.

2 Taken

2.1 Kwalificatieproces van de systeemkriticiteit

Zorgt ervoor dat elk industrieel controlesysteem dat zich in een aankoopproces bevindt, over een gekwalificeerd kriticiteitsniveau beschikt, zoals vastgesteld via de Engie Security Risk Assessment Methodology en bijgevolg in regel met de IEC 62443-2-4 conformiteitsvereisten (formeel de WIB **PROCESS CONTROL DOMAIN – SECURITY REQUIREMENTS FOR VENDORS Version II)**, zoals aangegeven in onderstaande tabel:

Systeemkriticiteitsniveau	Overeenstemmend IEC 62443 conformiteitsniveau
Kriticiteitsniveau van **9.0** of hoger	Conformiteitsniveau “goud”
Kriticiteitsniveau van **7.0** tot **8.99**	Conformiteitsniveau “zilver”
Kriticiteitsniveau onder **7.0**	Conformiteitsniveau “brons”

2.2 Aankoopproces

Ziet erop toe dat contracten voor procescontrolesystemen alle vereisten inzake informatieveiligheid bevatten en dat leveranciers de IEC 62443 conformiteitsmatrix invullen om het overeenkomstige conformiteitsniveau van het systeem aan te geven.

3 Beschrijving

3.1 Producten en diensten

Procescontrole- en automatiseringssystemen van leveranciers moeten beantwoorden aan de hierboven opgesomde vereisten (zie ondersteunende documenten) inzake ethische praktijken, normen en veiligheidsmaatregelen die bij de uitrol, het onderhoud en de werking van de infrastructuur moeten worden nageleefd.

ICS Security Compatible oplossingen dragen bij tot een hoog veiligheidsniveau maar moeten worden aangevuld met bijkomende veiligheidscontroles; bijvoorbeeld, aangepaste werkprocedures, vaardigheden & competenties van personeel, toegang van op afstand en algemene bestuurs- en managementpraktijken.

Om voor de hand liggende praktische en organisatorische redenen verbinden alle werknemers van leveranciers en hun onderaannemers zich ertoe om de veiligheidsmaatregelen en –normen van ENGIE na te leven. Concreet komt dit erop neer dat ze enkel software mogen leveren die aan deze normen beantwoordt en dat ze bij de ontwikkeling van die software enkel instrumenten en werkmethodes mogen gebruiken die overeenstemmen met de normen die ENGIE heeft aanvaard.

Het verholen gebruik van normen die niet aan de normen van ENGIE beantwoorden of die malware bevatten, zal worden beschouwd als een wezenlijke inbreuk waarvoor ENGIE een schadevergoeding van de leverancier kan eisen.

3.2 Personeel van de leverancier

Elke leverancier zal onder zijn medewerkers die met de uitvoering van een order zijn belast, een projectverantwoordelijke aanduiden die de activiteiten van zijn medewerkers zal superviseren en zijn gezag van werkgever over hen zal uitoefenen.

Wanneer de diensten volledig of gedeeltelijk in de kantoren van ENGIE worden verleend, zullen de medewerkers van de leverancier en die van zijn onderaannemers aan wie de dienstverlening is toevertrouwd, zich te allen tijde schikken naar de interne voorschriften van ENGIE inzake veiligheid en welzijn op het werk.

Wanneer de diensten volledig of gedeeltelijk worden verleend op computers die eigendom zijn van ENGIE of door haar worden geleased, en ongeacht of deze computers al dan niet met het netwerk van ENGIE zijn verbonden, zullen de medewerkers van de leverancier en die van zijn onderaannemers aan wie de dienstverlening is toevertrouwd, zich te allen tijde schikken naar de interne veiligheidsvoorschriften en ICS veiligheidsvereisten die bij ENGIE in voege zijn. De leverancier zal erop toezien dat deze documenten in het bezit worden gesteld van zijn medewerkers en door laatstgenoemden strikt zullen worden nageleefd. Indien de medewerkers van de leverancier de voorschriften, zoals vervat in voornoemde documenten, negeren of op welke wijze ook overtreden, zal de leverancier volledig aansprakelijk zijn voor elke daaruit voortvloeiende schade die ENGIE zou worden berokkend.

4 Ondersteunende en hulpdocumenten

Process Control Domain Security Requirements for Vendors IEC 62443. Het Excel-bestand met de IEC 62443 conformiteitsmatrix kan worden opgevraagd bij het aankoopdepartement en moet door leveranciers van industriële controlesystemen worden ingevuld.

5 Verklaring voor wijziging

Versienr	Reden van wijziging	Gewijzigde pg
00	Nieuw document	Alle
01	Wijziging van het document	Pagina 2-3