Publiek-Privaat samenwerkingsverband lanceert Security Check Procesautomatisering

Realisatie tool ter vergroting van cyberweerbaarheid OT-omgevingen

Den Haag, 5 juli 2021

Een Publiek-private samenwerking tussen het Ministerie van Economische Zaken en Klimaat (EZK), Digital Trust Center (DTC), Deloitte, VNG-IBD, Novel-T, NCSC, Siemens, ASML, Accenture en de Cybersecurity Alliantie, die belangen behartigt op het gebied van cyberveiligheid in operationele techniek (OT), introduceert vandaag de Security Check Procesautomatisering. Dit is een interactieve zelfscan die is ontwikkeld om Nederlandse organisaties met ICS-SCADA systemen handvatten te bieden in het weerbaarder maken van deze systemen. Het samenwerkingscollectief presenteert de tool aan Hester Somsen, plaatsvervangend Nationaal Coördinator Terrorismebestrijding en Veiligheid en aan Jos de Groot, directeur van de Directie Digitale Economie van het ministerie van Economische Zaken en Klimaat.

Weerbaarheid industriële controlesystemen

De Security Check Procesautomatisering lanceert een week na publicatie van het jaarlijkse Cybersecuritybeeld Nederland (CSBN) rapport, waarin opnieuw de kwetsbaarheid van de Nederlandse digitale infrastructuur centraal staat. De check biedt organisaties een praktische tool om invulling te geven aan de oproep uit het CSBN om de cyberweerbaarheid te vergroten en is het inspanningsresultaat van een uniek samenwerkingsverband. Dit ICS-samenwerkingsverband is eind 2019 ontstaan uit de werkgroep ICS Security binnen de Cybersecurity Alliantie en gevormd om organisaties (klein, groot, vitaal en niet-vitaal, privaat en publiek) belangeloos te helpen om de bewustwording te vergroten en hen concrete, toepasbare oplossingen te bieden waarmee de cyberweerbaarheid van hun industriële controlesystemen kan worden verbeterd. Omdat de Cybersecurity Alliantie een cruciale rol heeft gehad in de ontwikkeling van de Security Check Procesautomatisering, neemt Hester Somsen de tool namens de Cybersecurity Alliantie in ontvangst.

Het DTC, dat vanuit het Ministerie van EZK ondernemend Nederland ondersteunt op het gebied van digitale veiligheid, faciliteert de Security Check Procesautomatisering via haar website. DTC-Relatiemanager Jacco van der Kolk: *“Ik ben bijzonder verheugd om een praktisch inzetbare zelfscan te kunnen bieden aan organisaties die gebruik maken van ICS of OT-apparaten. De diversiteit in security-volwassenheid binnen dit ICS-domein is groot; Er zijn organisaties die zeer volwassen zijn maar ook organisaties die de digitale weerbaarheid van hun ICS-landschap flink moeten verhogen, maar helaas niet de kennis in huis hebben om dat te bewerkstelligen. Ik hoop dat wij met deze tool al deze organisaties kunnen helpen.”*

Praktisch hulpmiddel

De bedrijfsvoering van de meeste organisaties is tegenwoordig, vaak zonder dat ze zich daarvan bewust zijn, sterk afhankelijk van automatiserings- en control systemen. Met de huidige trend van digitalisering wordt dat eerder meer dan minder. Helaas neemt de kans op een cyberincident hierdoor ook toe. Met de Security Check Procesautomatisering kunnen organisaties snel in kaart brengen waar mogelijke risico’s zitten, maar ook welke beschermingsmaatregelen zij hiertegen kunnen nemen. De security check, die ook zonder technische of IT-kennis kan worden gebruikt, biedt organisaties een praktisch hulpmiddel om hun cyberweerbaarheid te vergroten.

Strategisch, tactisch en operationeel niveau

De cyberweerbaarheid van OT-omgevingen is heel specifiek omdat de industriële procesautomatisering binnen organisaties veelal een aparte digitale omgeving is en de beveiliging van de controlesystemen (ICS) om een andere aanpak vraagt dan IT-omgevingen. Hierdoor worden

de mogelijke risico's onderschat en is er nog onvoldoende ICS-veiligheidsbewustzijn. Om de juiste digitale weerbaarheidsmaatregelen te kunnen treffen is extra aandacht vereist, op zowel strategisch als tactisch en operationeel niveau. De Security Check Procesautomatisering draagt bij aan het verkrijgen van dit inzicht. In de check komen onderwerpen als toegangscontrole, incident respons en wijzigingsbeheer naar voren en zijn bestaande raamwerken, leidraden en normenkaders (bewezen methodieken en instrumenten) meegenomen als onderdeel van de route die door een organisatie afgelegd kan worden.

De risico-lat
Hoeveel en welke maatregelen een organisatie moet treffen hangt af van de gevolgen die er zijn als zich een cyberincident voordoet op de eigen industriële processen. Als de gevolgen ernstig zijn in financieel opzicht, er gezondheidsrisico's dreigen, of indien er ernstige milieuschade kan ontstaan, dan zijn de beschermende maatregelen die nodig zijn talrijker. De check begint dan ook met het inventariseren van een normkader; hoe hoog moet de risico-lat bij een organisatie liggen? Vervolgens biedt de tool het inzicht of de belangrijkste maatregelen worden getroffen om de ICS-omgeving te beschermen tegen cyberincidenten. Uitkomst van de Security Check Procesautomatisering is een checklist met maatregelen die passen bij het beveiligingsniveau van de organisatie.

In september zullen de eerste bevindingen rondom de inzet van de tool worden gepresenteerd door de ICS-alliantie tijdens de jaarlijkse cybersecurity conferentie ONE in Den Haag.

Over het ICS-samenwerkingsverband
Het Publiek-Private samenwerkingsverband op het gebied van cyberveiligheid in operationele techniek (OT) is ontstaan in 2019. Het doel van het samenwerkingsverband is het delen van kennis en het ontwikkelen en beschikbaar stellen van hulpmiddelen om bij te dragen aan een cyberweerbaar Nederlands bedrijfsleven, met bijzondere aandacht voor organisaties binnen het Nederlandse ICS-domein. Het samenwerkingsverband bestaat uit de volgende deelnemers:

Cybersecurity Alliantie
VNG
Programma Versterken Cyberweerbaarheid in de watersector
SIEMENS
accenture
ASML
Deloitte.
NovelT
National Cyber Security Centre
Ministry of Security and Justice
digital trust center.
STARK NARRATIVE