Program

Cyber- og informationssikkerhed i forsyningssektoren

Torsdag den 26. september 2019, kl. 10.00-15.30

Hos Kamstrup, Industrivej 51, Stilling/Skanderborg

Forsyningssektorens sårbarhed over for cybertruslen udvikler sig hastigt i takt med, at digitalisering af produktions-, distributions- og forbrugssiden tager til. Cybersikkerhed er en opgave, der udfordrer forsyningsselskabernes kerneforretning. Den fordrer et tæt og fortroligt samarbejde med ikke mindst leverandører, som skal levere *security by design* i deres løsninger og bidrage til at opretholde en høj sikkerhed, også når komponenter er installeret og ældes.

Denne workshop tager afsæt i "Cyber- og informationssikkerhedsstrategi for energisektorerne" (2019), som Klima-, Energi- og Forsyningsministeriet har udarbejdet i samarbejde med bl.a. Dansk Energi, Energinet og Dansk Fjernvarme.

Kl. 09.30	Registrering, morgenmad og netværk
Kl. 10.00	Introduktion til dagens program v. Henrik Martens, iEnergi
Kl. 10.05	Velkomst v. formand for Det smarte net Lars Hansen, Siemens og v. direktør, Kamstrup
Kl. 10:15	Cyber- og informationssikkerhed i Herning Vand – fra strategi til handling v. Poul Schlosser, administrationschef, Herning Vand
Kl. 10.45	Cyber- og informationssikkerhed i forsyningssektoren – fra strategi til handling v. Peter Kjær, chefkonsulent, Dansk Energi *Præsentation af Klima-, Energi- og Forsyningsministeriets strategi med fokus på de tre initiativer:* - *Krav til leverandørforhold (initiativ 3): Security by design - Hvilke krav bør en kunde stille til en leverandør? Og koster (øget) sikkerhed altid ekstra? Sikkerhed i clouden?* - *Sikring af digitale komponenter - IoT (initiativ 7): Hvordan kan vi – forsyningsselskab og leverandør – i fællesskab hæve sikkerheden for digitale komponenter og systemer?* - *Standarder og "best practices" (initiativ 8): Hvordan kan vi opretholde en høj sikkerhed, når komponenter er installeret og kun bliver ældre? Herunder legacy problematikken.*

Kl. 11.15	Kort pause

<u>Session 1 – Security by design:</u> Hvilke løsninger er sikre? Skal man in-source eller uddelegere sikkerhedskompetencer? Hvilke sikkerhedskompetencer kræver det in-house? Hvad kan uddelegeres?

Kl. 11:30	Security in Digital Transformation v. Carsten Horst, IBM
Kl. 12.00	Measuring cyber resilience of providers for critical infrastructure, case example from Finland v. Laura Noukka, F-Secure
Kl. 12:30	Frokost

<u>Session 2 - Samarbejde:</u> mellem forsyning og leverandør om sikkerhed: Hvad gør forsyningsselskaberne? Og hvad kan leverandørerne hjælpe med? Vi vil med denne del af programmet give nogle eksempler på det eksisterende samarbejde, der er mellem forsyningsselskaber og leverandører.

Kl. 13:15	Radius og Kamstrups samarbejde om målerudrulning m.m. v. Jørgen Fangel, Radius, og en produktspecialist fra Kamstrup
Kl. 13.45	Cerius og DTU's/Echelon's samarbejde om at hacke målere mv. v. Bo Danielsen, Cerius
Kl. 14.15	Experiences in securing IoT protocol standards: perspectives for the Danish energy sector v. Alessandro Bruni, IT-Universitetet
Kl. 14.45	Kaffe, kage og luft i lokalet

<u>Session 3 - Legacy problematikken</u>: Hvordan sikrer man efterfølgende, at sikkerheden holder det høje niveau, når "det nye udstyr" er installeret", og verden omkring os udvikler nye metoder til at trænge igennem.

Kl. 15:00	Hvordan håndteres Cyber Security i industrien? - hvilke standarder er fremherskende? - hvordan håndterer man legacy systemer, patching, overvågning, m.m.? v. Lars Peter Hansen, Technology Specialist Manager, Siemens
Kl. 15.30	Opsamling på dagens hovedpointer og afrunding v. Henrik Martens, iEnergi