CASE

I cybersikkerhedens tjeneste

Nye standarder indenfor IoT skal værne om cybersikkerheden for produkter og udstyr, der kobles på internettet. FORCE Technology's ajourførte viden om standarderne hjælper produktudviklerne på sikker vej.

Internet of Things (IoT) breder sig med lynets hast og stadig flere produkttyper og produktionsudstyr bliver tilsluttet internettet. Problemet er, at der på nuværende tidspunkt ikke stilles krav om cybersikkerhed, når produkter og udstyr kobles på internettet. Det er op til producenterne selv at vurdere sikkerhedsaspektet, og mange stiller forståeligt nok spørgsmålet "Hvornår er det sikkert nok, det vi gør?"

For it-systemer, computere, netværk og servere findes der allerede en række standarder for cybersikkerhed. Til gengæld er det mere mangelfuldt, hvad angår standarder til operationsudstyr som fx videoovervågning, procesanlæg, ventilationsanlæg og produktionsapparater. Områder hvor det bliver stadig mere vigtigt at stille krav til cybersikkerhed i form af adgangskontrol, softwareopdateringer og overvågning.

Nye regler på vej

ENISA (European Network and Information Security Agency) er i færd med at udarbejde cybersikkerhedsregler for produkter med indbygget datakommunikation. ENISA-reglerne forventes først at være klar i år 2023.

"P.t. ved vi ikke så meget om indholdet i de kommende regler andet end, at de vil indeholde krav til produkternes cybersikkerhed - krav som producenterne skal forholde sig til. Når reglerne er offentliggjort, vil der blive arbejdet på at finde relevante standarder, der kan bruges til krav-compliance fx ISO 62443-standarderne," fortæller specialist i cybersikkerhed, Jeppe Pilgaard Bjerre, FORCE Technology.

Til dagligt arbejder han med cybersikkerhed og vejleder kunder om, hvordan de kan beskytte deres IoT-produkter mod cyberangreb.

"I Danmark er vi meget tillidsfulde og forventer ikke, at folk udnytter os, men det bliver mere og mere vigtigt at tage højde for cybersikkerhed i takt med, at stadig flere produkter og produktionsudstyr bliver koblet op på internettet og derved potentielt bliver mere sårbare for cyberangreb."

Jeppe Pilgaard Bjerre, Specialist, FORCE Technology

Følger med via standardiseringsarbejdet

For Jeppe Pilgaard Bjerre er det essentielt at følge med i, hvad der sker på området for cybersikkerhed, så han kan give den bedste rådgivning til kunderne. Derfor er han medlem af ISO/IEC JTC 1/SC 41 "Internet of Things" (som også omfat-

FORCE Technology
Jeppe Pilgaard Bjerre
Specialist i cybersikkerhed

ter cybersikkerhed) og med i Dansk Standards S840-udvalg "Internet of Things".

"I S840-udvalget arbejder vi på at få ensartet billede af, hvordan cybersikkerheden er og skal være. Standarderne skal omfatte, hvad producenterne som minimum skal gøre for at sikre cybersikkerhed og lukke for de mest almindelige sårbarheder. Udvalget kigger ikke på ting som patientsikkerhed eller banksikkerhed. Fokus er mere på at finde laveste fællesnævner, fx ikke for simple passwords som nemt kan hackes, så man så vidt muligt undgår eksempelvis DDoS-angreb (Distributed Denial of Service). Den slags cyberangreb har lagt store firmaers hjemmesider ned de seneste par år," fortæller Jeppe Pilgaard Bjerre.

Udfordringen

På et område, hvor teknologien udvikler sig rygende hurtigt, er det en konkret udfordring at udvikle standarder om cybersikkerhed:

"Man skal passe på, at standarden ikke bliver for specifik, hvis nu teknologien udvikler sig i helt anden retning. Vi skal heller ikke stille alt for specifikke krav, som virker begrænsende for produktudviklerne."

En af de ting, som Jeppe Pilgaard Bjerre gerne vil italesætte i sit standardiseringsarbejde, knytter sig til, hvordan virksomheder kan opdage it-sårbarheder i deres produkter og udstyr:

"Når du markedsfører et nyt produkt, er det en rigtig god idé at oprette en kommunikationskanal, hvor brugerne kan rapportere tilbage til dig, hvis de har opdaget sårbarheder i dit produkt. På den måde kan vi I fællesskab højne sikkerhedsniveauet i Danmark."

Fakta

Screening for cybersikkerhed
Når FORCE Technology hjælper virksomheder med at foretage cybersikkerhedsscreening af nye IoT-produkter, omfatter det typisk risikovurdering og test for ekstern indtrængning, sårbarhed, software-svagheder og malware.

IoT
Anvendelsen af IoT-teknologien er i hastig udvikling. I 2016 var der på verdensplan omkring 7 milliarder IoT-enheder opkoblet til internettet. I 2020 forventes der ifølge analysefirmaet Gartner at være omkring 25 milliarder IoT-enheder.