# Titel: Styrkelse af dansk IoT-sikkerhed

**Institut: Alexandra Instituttet, Force Technology, DBI**

**Kontaktperson: Gert Læssøe Mikkelsen, Head of Security Lab, gert.l.mikkelsen@alexandra.dk**

## 0. Kort introduktion

Cybersikkerhed er en stigende udfordring for alle europæiske virksomheder, og dårlig IoT-sikkerhed er en trussel både for ejeren af et produkt og for alle andre. I 2016 blev dette tydeligt, da Mirai-angrebet via IoT-enheder med dårlig sikkerhed lagde mange tjenester på internettet ned. Der findes services og standarder på området, men de er ofte branchespecifikke eller nicheorienterede, og er ikke bredt accepteret til hverken industri- eller forbrugerprodukter.

EU har foreslået frivillige krav om certificering af IKT-produkter, og der begynder at komme standarder som f.eks. UL2900-1, IEC 62443 og ISO/IEC 27034. European Cyber Security Organisation (ECSO) har afdækket, at der findes ca. 290 standarder, som omhandler cybersikkerhed. Det viser, at alene mængden gør det vanskeligt for virksomheder at vide, hvilken de skal efterleve.

Dette forslag vil sikre, at GTS-netværket i fællesskab kan levere hjælp til at kortlægge standardiserede krav til virksomheders cybersikkerhed inden for IoT og dokumentere disse. FORCE Technology vil levere den nødvendige akkrediterede cybersikkerhedsscreening af produkter. Alexandra Instituttet vil levere de nødvendige it- og IoT-sikkerhedsservices. DBI – Dansk Brand- og sikringsteknisk Institut vil levere awareness-ydelser og branchespecifikke ydelser til domænet brand og sikring.

## 1. Markeds- og samfundsbehov

I oktober 2017 udkom første bud på en fælles EU-strategi for cybersikkerhed i IKT-produkter –i form af Cybersecurity act (yderligere uddybet af ENISA), en opfølgning på kravene til kritisk infrastruktur fra NIS direktivet. Dette er en frivillig ordning men en anerkendelse af behovet for en koordineret indsats. I december 2016 udstedte Food and Drug Administration (FDA) Postmarket Management of Cybersecurity in Medical Devices-guidelines. Deloitte, Alexandra Instituttet og Innovationsfonden udgav i marts 2018 rapporten The future market for cybersecurity in Denmark, som peger på brugernes kompetencer, sikre kanaler og security by design som de vigtigste punkter i sikringen af IoT-produkter, og der peges på et IoT-marked, der vil stige eksponentielt de kommende år. Regeringens Strategi for Danmarks digitale vækst (2018) udnævner it-sikkerhed som ét af de seks strategiske mål. Danske virksomheder skal styrkes på området, og det beskrives, at der skal udvikles værktøjer, der understøtter virksomhederne, ligesom GTS-institutternes rolle som støtter til SMV'erne og deres produktion beskrives.

I dag bliver virksomhedernes produkter mødt af mange forskellige krav, og det kan være svært at vide, hvilke standarder de skal udvikle til. Det er derfor essentielt at følge med i udviklingen i EU og levere ydelser til de danske virksomheder som producerer produkter til det europæiske marked.

Arbejdet med standarder og akkrediteringer er komplekst og ofte forbundet med et stort arbejde, som SMV'er kan have svært ved at allokere ressourcer til. En del af projektet vil derfor bestå i at afdække, hvorledes mindre virksomheder effektivt kan arbejde med relevante standarder.

Projektet henvender sig til virksomheder, som gerne vil have et professionelt forhold til cybersikkerhed, både producenter af IoT og smarte produkter, og virksomheder der baserer deres produktion eller forretning på anvendelse af IoT-produkter.

**2. Ny teknologisk serviceydelse, kompetence og teknologi**

På tværs af de tre GTS-institutter vil der blive udviklet rådgivnings- og akkrediteringsydelser inden for IoT og brugen af IoT-produkter.

- Rådgivning i forbindelse med valg af standarder og akkrediteringer og belysning af krav i pågældende standarder.
- Penetrationstestning og kodereview til afdækning af sårbarheder i produkter i henhold til relevante standarder.
- Rådgivning i forbindelse med etablering af en organisatorisk struktur for sikker udvikling af produkter – Secure Development Life Cycle.
- Auditeringsservice til virksomheder, så de forsat kan opretholde den specificerede cybersikkerhed, også i fremtidige produkter.
- Udvikling af framework for awareness-program.
- ISO 27001 akkrediteringsaudit.

Produkttests tager udgangspunkt i ydelser omkring standarden UL2900-1, men bliver udbygget til IEC 62443 og andre relevante standarder.

Mangel på konkrete standarder gør det svært at sammenligne cybersikkerhedsydelser og IoT-produkters sikkerhed og svært for virksomheder at komme i gang. Derfor vil dette forslag opstille konkrete mål, hvor indsatsen står mål med risikoprofilen for produktet, og ud fra standarder udvikle akkrediterede evalueringsmetoder for cybersikkerhed på produkt-, backend- og applikations-niveau samt for organisationen og dennes processer. Ydelserne bliver udviklet i fællesskab med udgangspunkt i de enkelte GTS-institutters kompetencer, som samlet giver endnu større værdi. Nogle ydelser bliver forankret hos de enkelte institutter, andre i fællesskab, blandt andet i Nordic IoT Center.

**3. Centrale aktiviteter**

Etablering af videnbase med udgangspunkt i standardiseringsorganisationerne ISO, IEC, ITU-T, ETSI og CEN/CENELEC. Dertil kommer kontakt med offentlige myndigheder som Center for Cybersikkerhed i Danmark og ENISA i Europa.

Internationale myndigheders holdning til cybersikkerhed og eventuel ny lovgivning kortlægges og perspektiveres til en dansk kontekst gennem dialog med dansk erhvervsliv, både producenter og brugere af IoT-enheder, og virksomheder der leverer cybersikring. Denne viden kombineres med den nuværende specialistviden hos de respektive GTS-institutter.

Dette vil blive suppleret af en gap-analyse af industrielle behov, idet ikke alle typer af cybersikkerhedscertificering kan dækkes af dette projekt. Kontakt til andre internationale leverandører af de mest specialiserede opgaver vil derfor blive etableret.

Derudover vil vi arrangere videnspredingsaktiviteter, blandt andet via IoT og Wirelessklubben og Nordic IoT Center.

**4. Mulige samarbejdspartnere**

- Virksomheder der anvender/udvikler IoT
- Leverandører til kritisk infrastruktur (elforsyning, transport og datakommunikation)
- Europæiske organisationer: AIOTI, ECSO, TDL, ENISA.
- Standardiseringsorganisationer: CENELEC, ISO/IEC, ITU-T
- Innovationsnetværkene i Danmark
- Cybersikkerhedsrådgivere i Danmark.

Alexandra Instituttet og FORCE Technology har allerede indgået et samarbejde i Nordic IoT centre, hvor det er tydeligt, at de kan stå stærkere sammen og sikre optimale løsninger, der sætter begge institutters kompetencer i spil. Dertil kommer naturligt DBI, som med deres sikringsviden er centrale i en holistisk tilgang til virksomheders sikkerhed og cybersikkerhed. Baseret på fælles erfaringer fra RK-projektet Sikkerheds- og privacyværktøjer, regnes dette samarbejde for den ideelle løsning for at dække hele bredden i udfordringen med at optimere cybersikkerheden i IoT-systemer.