# Skema: Ansøgning om resultatkontraktmidler 2019-2020

| **Institut(ter):** | **Aktivitetsplan (titel):** | **Aktivitetsplan nr.: 9** | **FoU** |
|---|---|---|---|
| Alexandra Instituttet<br>FORCE Technology<br>DBI | Styrkelse af dansk IoT-sikkerhed<br><br>**Idéforslags titel på bedreinnovation.dk:**<br>Styrkelse af dansk IoT-sikkerhed | | |

## 1) Manchettekst (kort resumé)

Danske virksomheder er internationalt kendt for deres kvalitetsprodukter. Dette brand skal bevares – også når produkterne gøres smarte og kobles på internettet. Det er derfor helt vitalt for danske virksomheder at have styr på IoT-sikkerheden.

## 2) Aktiviteten kort (resumé)

IoT-sikkerhed er en stigende udfordring for alle virksomheder, der bruger IoT i infrastruktur og produkter. Det er derfor vigtigt, at danske virksomheder har kompetencerne til at kunne vælge sikre IoT-løsninger, og at danske producenter har kompetencerne til at udvikle og producere sikre IoT-produkter. Det er vigtigt at opretholde det brand omkring kvalitet, som danske produktionsvirksomheder generelt har. En amerikansk undersøgelse har vist, at dårlig IoT-sikkerhed har direkte økonomiske konsekvenser for virksomhederne, og at brand og omdømme er de vigtigste parametre, når virksomheder skal vælge IoT-sikkerhedsløsninger.[1]

Center for Cybersikkerhed (CfCS), vurderer truslen for cyberspionage og -kriminalitet til at være meget høj[2], både generelt for danske virksomheder og mod konkrete sektorer, senest sundhedssektoren[3], hvor også truslen fra dårlig IoT-sikkerhed fremhæves. Dårlig IoT-sikkerhed er en trussel for:

1. Den enkelte borger eller virksomhed i form af læk af følsomme personlige eller virksomhedsdata.
2. Ejeren af produktet, i form af f.eks. en infrastruktur der ikke virker. I 2016 mistede 900.000 Deutsche Telecom-kunder adgang til internettet direkte på grund af dårlig IoT-sikkerhed[4].
3. Samfundet. Et lignende angreb gjorde visse dele af internettet utilgængeligt i 2016[5].
4. Producenten af produktet, som bliver valgt fra på grund af dårlig sikkerhed.

Nogle danske virksomheder tager heldigvis denne udfordring alvorligt og arbejder i stigende grad på at forbedre IoT-sikkerheden i deres produkter, men der er brug for at få alle med. Desuden er der mange danske produktionsvirksomheder, der først nu eller i de kommende år vil begynde at forbinde deres produkter til internettet og gøre dem smarte. Det er vigtigt, at de også har fokus på IoT-sikkerheden.

Målgruppen for denne aktivitet er bred men er hovedsageligt produktionsvirksomheder inden for SMV-segmentet. Mange af disse virksomheder er i disse år i gang med at digitalisere både produktion og produkter, og mange af disse virksomheder er leverandører til sektorer, hvor der kommer krav omkring sikkerhedsniveauer. Det gælder både inden for kritisk infrastruktur (NIS[6] direktivet) og i f.eks. bygningsreglementet. For at sikre et tilstrækkeligt niveau af IoT-sikkerhed i forhold til truslerne, og for at kunne dokumentere dette, er det nødvendigt for virksomhederne at kigge på standarder og certificeringer.

Der findes allerede guides og standarder på området, men de er ofte branchespecifikke eller nicheorienterede og ikke bredt accepteret til hverken industri-eller forbrugerprodukter. EU har foreslået frivillige krav

[1] Are your company's IoT devices secure?, Altman Vilandrie & Company, Juni 2017, http://www.altvil.com/wp-content/uploads/2017/06/AVCo.-IoT-Security-White-Paper-June-2017.pdf
[2] Cybertruslen mod Danmark, Center for Cybersikkerhed/FE, maj 2018.
[3] Cybertruslen mod sundhedssektoren, Center for Cybersikkerhed/FE, juli 2018
[4] https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/
[5] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
[6] http://horten.dk/Viden/Artikel%202016/NIS-direktivet-stiller-nye-krav-til-sikkerhed-i-net-og-informationssystemer

om certificering af IKT-produkter, og der begynder at komme standarder som f.eks. UL2900-1, UL2900-2, IEC 62443 og ISO/IEC 27034. Mange af disse standarder er dog forholdsvis omfattende – hvilket er en hindring specielt for opstarts- og mindre virksomheder[7][8]. Samtidig har European Cyber Security Organisation (ECSO) afdækket, at der findes ca. 290 standarder, som omhandler sikkerhed i bred forstand[9]. Det viser, at alene mængden af generelle standarder gør det vanskeligt for virksomheder at vide, hvilken de skal efterleve inden for deres sektor.

Denne aktivitetsplan vil sikre, at GTS-institutterne i fællesskab er i stand til at levere ydelser og hjælp til at kortlægge standardiserede krav til virksomheders cybersikkerhed omkring både brug og udvikling af IoT-produkter samt dokumentere disse krav. Dette bliver opfyldt via følgende to hovedaktiviteter:

1. Skabe overblik over standarder og krav, blandt andet ved desk research og konferencedeltagelse samt ved deltagelse i internationale organisationers arbejde og standardiseringsarbejde omkring IoT-sikkerhed. Både for at medvirke til, at de relevante standarder kommer til at passe med danske virksomheders (herunder SMV'ers) behov, og for at hente viden hjem og kunne certificere virksomheder og produkter ud fra relevante standarder. Dette er kontinuert arbejde, der vil række ud over projektperioden på to år, men denne aktivitet vil sikre, at vi kan komme i gang med at udvikle ydelser og kommer hurtigt ind i standardiseringsarbejdet på området.

2. Udarbejde guides og best practice-beskrivelser rettet mod virksomhederne, så de nemt kan få oversigt over relevante standarder, og i hvilken grad de kan leve op til dem. Best practice-beskrivelserne vil blandt andet blive udarbejdet på baggrund af de virksomheder, der allerede arbejder med IoT-sikkerhed.

**Output fra aktivitetsplanen:**
Output vil være rådgivningsydelser men i højere grad evaluerings- og certificeringsydelser. Via rådgivningsydelserne vil GTS-institutterne kunne hjælpe virksomhederne med at højne deres IoT-sikkerhed og udvikle sikrere produkter samt give dem viden om, hvilke standarder der er relevante for dem, og hvad der skal til for at leve op til dem. Via evaluerings- og certificeringsydelserne vil GTS-institutterne kunne evaluere og certificere, at virksomhederne lever op til relevante standarder, således at virksomhederne kan dokumentere dette over for både kunder og myndigheder.

### 3) Markedsbehov, erhvervs- og samfundsmæssige potentialer

Markedet for IoT er i disse år eksponentielt stigende, og det er vigtigt at sikre, at danske virksomheder kan være med i denne vækst. Danmark er et af de mest digitaliserede lande i verden, vi er verdensmester i offentlig digitalisering[10], og vi er et af de OECD-lande, der har flest IoT-enheder pr indbygger[11]. Dårlig IoT-sikkerhed kan dog være en hæmsko for dette marked, så det er vigtigt at kunne hjælpe danske SMV'er med at have styr på IoT-sikkerheden og kunne dokumentere dette via certificeringer.

FORSK2025 påpeger, at IT- og IoT-sikkerhed er en forudsætning for at kunne udnytte fremtidens digitale muligheder, og at sikkerhed kan blive et konkurrenceparameter for Danmark. Dette stemmer overens med en rapport[12] udgivet i år af Alexandra Instituttet, Deloitte og Innovationsfonden, der viser, at Danmark har et stort potentiale som leverandørland inden for cybersikkerhed, herunder IoT-sikkerhed. I undersøgelsesfa-

[7] https://www.networkworld.com/article/2199260/compliance/cost-of-regulatory-security-compliance--on-average---3-5m.html
[8] https://www.computerweekly.com/feature/Tackling-the-IT-security-and-compliance-challenges-for-SMEs
[9] https://www.ecs-org.eu/working-groups/news/wg1-state-of-the-art-syllabus-updated
[10] https://www.fm.dk/nyheder/pressemeddelelser/2018/07/dk-verdensmester-i-digitalisering
[11] Consumer Product Safety in the Internet of Things. OECD, 2018
[12] The Future Market for Cybersecurity in Denmark, Alexandra Instituttet, Deloitte, Innovationsfonden, 2018, https://innovationsfonden.dk/sites/default/files/thefuturemarketforcybersecurityindenmark.pdf

sen til rapporten fik vi fra danske virksomheder, der arbejder med cybersikkerhed, kommentarer som: *"Manufacturers are not good at thinking about security and privacy when developing products"* og *"The Internet of Things is a setback for cybersecurity"*.

Det er vigtigt, at vi får vendt dette billede, så danske virksomheder bliver kendt for at levere kvalitetsprodukter, også når de digitaliserer produkterne, som beskrevet i en af kommentarerne på Bedreinnovation.dk: *"Der er behov for at sikre, at danske IoT-produkter bliver brandet som sikre på den internationale markedsplads. Vi skal have Danish Security op på linje med Danish Design fra 60'erne og 70'erne. Dertil er der brug for at læne sig op ad internationale certificeringer, som kan bruges til at signalere god sikkerhed. Der er behov for, at virksomhederne kan få adgang til en let tilgængelig oversigt over den urskov at standarder der findes. Der er ligeledes behov for, at især de mindre og stærkt specialiserede virksomheder kan få hjælp til, hvordan de skal komme igennem certificeringerne. Dette projekt vil være en stor hjælp for dansk erhvervsliv over en bred kam, og det er derfor meget velkomment."* Henning Mortensen, formand for Rådet for Digital Sikkerhed og CISO/CPO ved Brdr. A&O Johansen A/S.

**Regulatoriske krav**
I dag bliver 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. 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. Det er på nuværende tidspunkt en frivillig ordning, der anerkender behovet for en koordineret indsats, men på sigt kan det blive et de facto krav i forbindelse med eksempelvis offentlige udbud. I december 2016 udstedte Food and Drug Administration (FDA) Postmarket Management of Cybersecurity in Medical Devices-guidelines[13]. Desuden er cybersikkerhed af kritisk infrastruktur en vigtig del af regeringens strategi for cybersikkerhed[14] (2018).

**Målgrupper**
Alle virksomheder har en interesse i at kunne dokumentere, at de og deres produkter lever op til forskellige krav med hensyn til sikkerhed. Dette kan være i forbindelse med at leve op til lovkrav eller en del af markedsføringen, hvor produktets sikkerhed kan garanteres. Eksempelvis vil NIS-direktivet stille øgede sikkerhedskrav til aktører inden for kritisk infrastruktur. Da disse aktører anvender en række underleverandører, vil underleverandørerne have et behov for at kunne dokumentere sikkerheden af deres produkter. Det samme gælder for leverandører til bygningsbranchen, da også bygningsreglementet er begyndt at indeholde krav om IoT-sikkerhed.

Den primære målgruppe for denne aktivitetsplan er danske produktionsvirksomheder, som benytter IoT i deres produktion, eller virksomheder der producerer produkter, der går fra at være fysiske produkter til også at være digitale smarte produkter, som er forbundet til internettet – en transformation en stor del af de danske produktionsvirksomheder enten er i gang med eller skal i gang med. Målgruppen er hovedsageligt SMV'er, men er ikke begrænset til dette segment. Vi forventer også, at større virksomheder vil have brug for de udviklede ydelser.

**Dialog med og efterspørgsel fra målgruppen**
I forbindelse med førnævnte rapport (The Future Market for Cybersecurity in Denmark[15]) gennemførte Alexandra Instituttet workshops og interviews med virksomheder (20 stk. af blandet størrelse), Dansk Industri, IT-brancheforeningen, forskere, Tænk (tidl. Forbrugerrådet) og flere offentlige institutioner. IoT-sikkerhed

[13] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
[14] National strategi for cyber- og informationssikkerhed, Regeringen, 2018.
[15] The Future Market for Cybersecurity in Denmark, Alexandra Instituttet, Deloitte, Innovationsfonden, 2018, https://innovationsfonden.dk/sites/default/files/thefuturemarketforcybersecurityindenmark.pdf

var et punkt, der blev vurderet som meget vigtigt for både samfundet og for virksomheder. Derudover er input fra rundbordssamtalerne i det nuværende RK-projekt "Sikkerheds- og privacyværktøjer" taget med i overvejelserne omkring denne aktivitetsplan. Desuden er certificering efter standarder og arbejdet med disse noget, som flere kunder og samarbejdspartnere har efterlyst i vores nuværende ydelser.

**4) Vidensprednin og inddragelse**

*Advisory Board (følgegruppe)*
For at sikre, at alle aktiviteter og mål for denne aktivitetsplan er relevante for målgruppen af virksomheder, vil der blive oprettet en følgegruppe. Den vil bestå af 8 personer fra relevante virksomheder. Da der arbejdes med standardiseringsarbejde og hjemtagning af kompetencer til Danmark inden for dette felt, vil følgegruppen være en fast gruppe for at sikre kontinuitet, og fordi det kræver et vist kendskab til standardiseringsarbejde. Der opnås herunder en afklaring af Alexandra Instituttets rolle ift. private rådgivere og leverandører mhp. at optimere synergi og komplementaritet og undgå konkurrenceforvridning.

*Vidensprednin*
En del af vidensspredningen vil foregå via GTS-institutternes allerede eksisterende netværk omkring IoT-udvikling og -anvendelse. Det vil blandt andet ske gennem IoT og Wireless-klubben, som drives af FORCE Technology (2 møder pr år) og via aktiviteter i Nordic IoT Center, som er et fællesskab mellem FORCE Technology og Alexandra Instituttet. Der vil også foregå vidensprednin gennem relevante fagmedier (3 publikationer pr. år, videnskabelige såvel som artikler i relevante danske fagmedier) og via faglige oplæg (4 pr. år) på danske eller udenlandske konferencer eller workshops. Vi vil via vidensspredningsaktiviteter (faglige oplæg og workshops) nå ud til 100 virksomheder i løbet af de to år.

*Casevirksomheder*
Udviklingen af ydelserne i dette projekt vil blive afprøvet på casevirksomheder undervejs. Dette sker både for at opbygge viden og erfaring hos GTS-institutternes, men i lige så høj grad for at sikre relevansen af de valgte standarder, der kan certificeres efter. På samme måde vil der blive samarbejdet med virksomheder omkring en best practice case mapping af arbejdet med IoT-sikkerhed i danske virksomheder. Der vil blive inddraget 8 casevirksomheder hvert år.

*Universitetssamarbejde*
I projektet vil vi forsøge at styrke universitetssamarbejdet, og der vil hvert år blive skrevet mindst en forskningsansøgning. Desuden vil vi forsøge at inddrage studerende på vej ud i erhvervslivet og styrke universitetssamarbejdet via samarbejde omkring kandidatprojekter.

*Samarbejde med innovationsnetværk*
Der vil blive samarbejdet med innovationsnetværkene, både InfinIT og Inno-Sec, der er meget relevante samarbejdspartnere i dette projekt. De tre GTS-institutter har allerede et godt samarbejde med InfinIT og Inno-Sec. Projektet være relevant for MADE (inkl. innovationsnetværket), hvor GTS-institutterne er repræsenteret. Der vil blive gennemført mindst 2 fælles aktiviteter pr. år med netværkene.

*Samarbejde med Industriens Fond*
Vi er i kontakt med Industriens Fond omkring et muligt samarbejde i aktivitetsplanen.

**5) Konkrete aktiviteter**

De overordnede mål er at skabe overblik over, hvilke IoT-sikkerhedsstandarder der findes og øge brugen af disse i danske virksomheder, især SMV'er. Dette opfyldes ved en række videnindhentende aktiviteter, som vil føde ind i ydelsesskabende og vidensprednde aktiviteter:

**Overblik over standarder og regulatoriske krav:**
ECSO har kortlagt over 290 forskellige standarder, der i bred forstand omhandler sikkerhed inden for IT. Samtidigt kommer der flere lovmæssige krav, eksempelvis GDPR eller NIS-direktivet, som også stiller krav

til sikkerheden. Dette gør det vanskeligt at bevare overblikket over, hvilke krav et produkt kan eller skal opfylde. Samtidigt er der få endelige standarder inden for specifikt IoT, men der er mange på vej. Det er medvirkende til at gøre det endnu mere uoverskueligt at finde den rigtige og mest relevante standard.
I denne aktivitet vil arbejdet med at skabe overblik tage udgangspunkt i offentlige myndigheder som Center for Cybersikkerhed i Danmark, ENISA i Europa og NIST internationalt niveau. Da der kan være særlige krav i forbindelse med specifikke brancher, såsom eksempelvis medico-udstyr, brand og sikring eller energisektoren, skal disse også undersøges. De 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 inden for IoT. Samtidig sikrer aktiv deltagelse i organisationer som CEN/CENELEC og ISO, at GTS-institutterne har mulighed for at komme med input til evt. nye standarder og best practice, hvilket sikrer, at der kan tages hensyn til danske forhold og ønsker. Denne viden kombineres med den nuværende specialistviden hos de respektive GTS-institutter og udbygges yderligere ved deltagelse i en række internationale organisationer f.eks. ECSO og OWASP og konferencer om IoT-sikkerhed.

Aktiviteten vil også omfatte screeninger af, hvordan danske virksomheder på nuværende tidspunkt arbejder med sikkerhed i IoT. Disse screeninger vil dels belyse, hvor modne danske virksomheder er inden for IoT-sikkerhed og kan bruges til at dokumentere de erfaringer, danske virksomheder har gjort sig på området, så andre virksomheder kan bygge videre på disse erfaringer. Dette arbejde vil munde ud i et eller flere white-papers, som kan hjælpe andre virksomheder med lettere at implementere et højt sikkerhedsniveau.
Endelig vil GTS-institutterne deltage i relevant forskning inden for området, for at sikre et fortsat godt kendskab til udviklingen inden for IoT-sikkerhed efter projektets afslutning, og for at sikre at ydelserne kan vedligeholdes.

**Udvikling af kompetencer og ydelser/services:**
Udviklingen af ydelser vil ske i tæt samarbejde med dansk erhvervsliv, både via projektets følgegruppe men i høj grad også via input fra screeninger og projektets mange case-samarbejder. Standarder kan være vanskelige at omsætte til praksis uden et stort fagligt kendskab til området. Det vil vi derfor hjælpe dansk erhvervsliv med. I samarbejde med følgegruppen, og de screeninger der er en del af aktivitetsplanens videnopbygning og -hjemtagning, vil der blive udarbejdet en eller flere guides til, hvordan kravene kan opfyldes af specielt SMV'er.

Samtidigt vil GTS-institutterne udvikle ydelser, der gør, at de kan certificere, at kravene i en given standard er opfyldt. I den forbindelse vil for de fornødne akkrediteringer blive hjemhentet, og relevante medarbejdere blive certificeret, således at de kan forestå arbejdet. Kontakt til andre internationale leverandører af de mest specialiserede opgaver vil også blive etableret. De konkrete ydelser er yderligere beskrevet i afsnit 6).

**Vidensprednin**g:
Samarbejdet med de internationale sikkerhedsorganisationer vil også resultere i nyeste viden om, hvilken retning sikkerhedsarbejdet bevæger sig i. Dette vil primært blive videreformidlet som faglige oplæg på relevante konferencer. Dialogen med danske virksomheder og vidensprednin**g** er yderligere beskrevet i afsnit 4)

## 6) Nyhedsværdi og ambitionsniveau

Alexandra Instituttet leverer allerede ydelser inden for blandt andet risikovurdering og sikkerhedstests af software-systemer og IoT-produkter. Ydelserne er baseret på mindre formelle, interne procedurer, hvilket skaber en intern værdi for kunderne i form af et mere sikkert produkt men begrænset værdi i forhold til kundens eksterne partnere. Et stigende antal kunder er derfor begyndt at efterspørge egentlig certificering af deres produkter.

Arbejdet med IoT-sikkerhed er nyt og er f.eks. nævnt som et vigtigt felt i FORSK2025. Inden for IoT-sikkerhed er der kun få og meget nye standarder, men der er mange på vej. Samtidig er der regulatoriske krav på vej, så området er nyt og bevæger sig derfor ud over de ydelser og certificeringer, GTS-nettet og andre

udbyder i dag. Der er derfor lige nu et allerede eksisterende behov for både de konkrete screeninger og certificeringer og for vejledning i forbindelse med, hvilke standardiserede krav, der kan være relevante. Det er en relevant opgave for GTS-nettet at udbyde certificeringer og arbejde med standarder – også inden for IoT-sikkerhed.

*"[…]Dansk Standard mener, at GTS'erne har en vigtig strategisk og operationel rolle i at deltage aktivt i udvikling af internationale/europæiske standarder på områder, som er af afgørende interesse for dansk erhvervsliv. Gennem internationale standarder kan GTS'erne effektivt opbygge og formidle teknologiske kompetencer til dansk erhvervsliv. GTS'erne er ofte i en unik situation, hvor deres brede kendskab til danske virksomheders behov og udfordringer, sætter dem i stand til at varetage danske interesser, når der udvikles nye internationale standarder. Dansk Standard oplever at GTS'erne er efterspurgte i standardiseringsarbejdet, da de bidrager med unik og aktuel viden, som efterspørges af virksomhederne."* Dansk Standard, kommentar på BedreInnovation.dk.

**Nye ydelser der kommer ud af projektet:**
I 2019 vil der blive udviklet og udbudt 3 ydelser: En akkrediteret cybersikkerhedstest af IoT-produkter; en lettere sikkerhedstest for IoT-systemintegration i forhold til bygningsreglementet; en lignende i et domæne defineret ud fra virksomhedernes behov.

I 2020 vil der blive udviklet og udbudt 3 nye ydelser: Auditering efter en relevant standard i ISO27000-serien for virksomheder, der arbejder med IoT; en ydelse om evaluering af compliance med NIS-direktivet og Cybersecurity act. (nye EU krav); samt en ydelse om hjælp med udvikling af IoT-produkter med høj sikkerhed (Secure Development Life Cycle) ,herunder patch management og segmentering af dele af produktet, der skal leve op til andre certificeringer. Dette gør, at produkterne kan fortsætte med at være sikre – også hvis de har en lang levetid, som f.eks. smartmålere og IoT-produkter til industrien.

**7) Vidensamarbejde og -hjemtagning**

Internationalt vil der blive taget viden hjem på følgende måder:

1. Desk research omkring output fra relevante organisationer, f.eks. amerikanske NIST, GSMA (GSM Alliance) og Europæiske ENISA. Desuden vil der blive fulgt med i EU-lovgivning på området.
2. Deltagelse i internationale konferencer og workshops.
3. Deltagelse i internationalt forskningssamarbejde. Alexandra Instituttet har lige ansøgt om EU-projektet SAFE[16] med internationale virksomheder og universiteter med viden inden for området. Der vil i projektet blive ansøgt om flere forskningsprojekter. Mindst et pr. år.
4. Deltagelse i internationale organisationers arbejde, blandt andet ECSO (European Cyber Security Organisation), det Europæiske TDL (Trust in Digital Life) og OWASP.
5. Deltagelse i standardiseringsarbejde, både i samarbejde med Dansk Standard samt arbejde i internationale standardiseringsorganisationer som CENELEC, ISO/IEC, ITU-T. Dette vil sikre både videnhjemtagning og dansk indflydelse på de udviklede internationale standarder til fordel for danske virksomheder.

**8) Sammenhæng med instituttets strategi og afsæt i instituttets ressourcer**

**Alexandra Instituttet A/S**
Både cybersikkerhed og IoT-sikkerhed er centrale fokusområder i Alexandra Instituttets strategi. Det er områder hvor Alexandra Instituttet vil udbygge både F&U-aktiviteter og i særdeleshed kommercielle services og ydelser. Denne aktivitetsplan vil være med til at styrke Alexandra Instituttets viden på området og samtidig sikre, at viden fra andre F&U-projekter, herunder EU-projekter, hurtigt kan komme dansk erhvervsliv til

[16] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ict-01-2018.html

gode i form af konkrete ydelser. Alexandra Instituttet har allerede i afdelingen Security Lab en klar spidskompetence inden for cybersikkerhed og IoT-sikkerhed – kompetencer der allerede udbydes i kommercielle ydelser. Der er dog stadig et stort behov for denne aktivitet for at opretholde og udvikle denne spidskompetence til også at dække de nyeste standarder og certificeringsordninger, så GTS-institutterne i samarbejde kan udbyde nye konkrete ydelser til dansk erhvervsliv baseret på den nyeste viden og især de nyeste standarder og certificeringsordninger inden for IoT-sikkerhed. Viden, kompetencer og ydelser udviklet under denne aktivitetsplan vil blive forankret i Alexandra Instituttets Security Lab samt i Nordic IoT Center, som Alexandra Instituttet har oprettet i samarbejde med Force Technology.

**FORCE Technology**
En byggesten for FORCE Technology er blandt andet at levere den teknologiske infrastruktur til blandt andet produktgodkendelser baseret på vores faciliteter. I tråd med strategien om Teknologisk Service 2.0, vil ydelserne i denne aktivitetsplan være fokuseret på at samlevere test sammen med DBI og Alexandra Instituttet. Samtidig vil ydelserne adressere Digitalisering 2.0, så vores kompetencer fra fysiske test bliver udvidet til også at omfatte det digitale domæne. Ydelserne tilstræber at understøtte virksomhederne i deres design og udvikling ved at dokumentere, at denne resulterer i de tilsigtede cybersikre løsninger. FORCE tjener i dag et stort segment af de kunder, der fokuserer på den danske styrkeposition om at skabe pålidelige kvalitetsprodukter, og det vil derfor være naturligt for disse at udvide med cybersikkerhed. Viden og kompetencer vil blive forankret gennem Nordic IoT Center i samarbejde med Alexandra Instituttet.

**Dansk Brand- og sikringsteknisk Institut**
Brand- og sikringsanlæg bliver i stigende omfang integreret med bygningsstyringssystemer. Samtidig bliver anlæggene koblet til internet gennem IoT-sensorer, ligesom der skal kunne gennemføres vedligeholdelse og overvågning udefra. Det skaber en række sårbarheder i virksomhedens fysiske sikkerhed. DBI har derfor et strategisk fokus på at opbygge kompetencer koblet til sårbarhed af IoT, så vi kan rådgive om forebyggelse, herunder henvise til specifik rådgivning hos Alexandra Instituttet og Force Technology.

**De tre GTS-institutter i samarbejde**
De tre GTS-institutter har hver især spidskompetencer inden for forskellige dele af IoT-sikkerhed. I samarbejde vil de tre GTS-institutter derfor kunne udbyde mere fuldendte løsninger. Alexandra Instituttet og FORCE Technology har allerede indgået et samarbejde i Nordic IoT Center, hvor det er tydeligt, at de kan stå stærkere sammen og sikre optimale løsninger, der sætter begge GTS-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.

## 9) Tidsplan og milepæle

**Milepæle 2019:**

*Vidensamarbejde, -hjemtagning og kompetenceopbygning*

1.1 Internationalt standardiseringssamarbejde, deltage i mindst 2 udvalg omkring standardisering.
1.2 Internationale organisationer inden for sikkerhed og standardisering, samarbejde med mindst 2 internationale organisationer.
1.3 Best practice case mapping af arbejdet med IoT-sikkerhed i danske virksomheder. Aktiviteten er baseret på undersøgelser hos casevirksomheder. Whitepaper om resultatet.
1.4 State-of-the-art cybersikkerhedscertificeringer. 3 medarbejdere (1 hos hvert GTS-institut) certificeret.
1.5 Mindst en forskningsansøgning.
1.6 Deltagelse i 1 internationale konference.

*Udvikling af teknologisk service (følgende ydelser udviklet med casevirksomheder og udbudt)*

1.7 Akkrediteret cybersikkerhedstest af IoT-produkter udbudt.

1.8 Ultra Light Assessment IoT System integration i forhold til bygningsreglementet
1.9 Ultra Light Assessment IoT System integration i domæne defineret ud fra danske virksomheders behov

*Inddragelse og vidensprednin*g
1.10 IoT og Wirelessklub – 2 møder
1.11 3 publikationer – dækker både videnskabelige publikationer samt artikler i relevante danske fagmedier (trykte eller online), mindst 1 per GTS-institut.
1.12 4 faglige oplæg på danske eller udenlandske konferencer eller workshops, mindst 1 pr. GTS-institut.
1.13 Følgegruppe rekrutteret, mindst 8 personer fra relevante virksomheder, både SMV'er og større virksomheder.
1.14 2 møder med følgegruppe.

**Milepæle 2020:**
*Vidensamarbejde, -hjemtagning og kompetenceopbygning*
2.1 Internationalt standardiseringssamarbejde, deltage i mindst 2 udvalg omkring standardisering (ikke nødvendigvis nye)
2.2 Internationale organisationer inden for sikkerhed og standardisering, samarbejde med mindst 3 internationale organisationer.
2.3 Mindst en forskningsansøgning.
2.4 Deltagelse i 1 internationale konference.

*Udvikling af teknologisk service (følgende ydelser udviklet med casevirksomheder og udbudt)*
2.5 Auditering for virksomheder der arbejder med IoT-systemer – efter standard i ISO27000-serien.
2.6 EU: NIS-direktivet + Cybersecurity act, compliance assessment
2.7 Rådgivning omkring Secure Development Life Cycle (inkl. patch management og segmentering)

*Inddragelse og vidensprednin*g
2.8 IoT og Wirelessklub – 2 møder
2.9 Rapport om regulatoriske cybersecuritykrav til IoT-produkter.
2.10 3 publikationer – dækker både videnskabelige publikationer samt artikler i relevante danske fagmedier (trykte eller online), mindst 1 pr. GTS-institut.
2.11 4 faglige oplæg på danske eller udenlandske konferencer eller workshops.
2.12 2 møder med følgegruppe.