Sikring af kritiske systemer og kritisk infrastruktur

A. INDLEDENDE OPLYSNINGER	
Aktivitetsområde	Indsatsområdet Digital sikkerhed, tillid og dataetik
Institut	Alexandra Instituttet
Titel *Dækker indholdet af aktiviteterne*	Sikring af kritiske systemer og kritisk infrastruktur
Nummerering *Af beskrivelsen*	4
Version	1
Periode *Forventet start og slut*	1/1 2021-31/12 2021
Kontaktperson	Kristian Krämer

B. ÆNDRINGER
Angiv her, hvis en planlagt aktivitet er ændret i forhold til den forudgående version af beskrivelsen.

C. BESKRIVELSE	
1. Mål *Hvorfor?* Hvad er målet for aktiviteterne? Hvordan bidrager de til det overordnede mål for aktivitetsområdet?	Både Danmark og andre lande er i gang med at digitalisere kritiske systemer og kritisk infrastruktur og forbinde dem til internettet. Det gælder rent digital kritisk infrastruktur, som vores samfund er afhængig af, men det gælder også fysisk kritiske systemer i vores virksomheder og fysisk kritisk infrastruktur, der digitaliseres. Dette gælder i særdelshed OT-netværk (operational technology, dvs. datanetværk i fabriks- og produktionsmiljøer modsat klassiske it-netværk), IoT-enheder samt samfundsmæssigt kritisk infrastruktur i f.eks. forsyningssektoren. Denne aktivitet vil både omhandle sikring af kritiske systemer i danske virksomheder og dansk kritisk infrastruktur, men vi vil hovedsageligt fokusere på at hjælpe danske virksomheder med at kunne levere produkter og tjenester til kritiske systemer og kritisk infrastruktur i både Danmark og udlandet. Både herhjemme og i udlandet er der øget fokus på cybersikkerheden i kritisk infrastruktur – bl.a. via NIS-direktivet[1] og cybersikkerhedsforordningen[2] Konkret vil dette aktivitetsområde bidrage til indsatsområdet overordnede mål med et eller flere nye samarbejder med vidensinstitutioner og en F&I ansøgning. Der vil blive arbejdet på teknologiske services, disse forventes dog først at være klar til markedet i en efterfølgende aktivitetsperiode.
2. Indhold *Hvad* skal der ske? Hvilke(n) konkret(e) aktiviteter udføres?	Kompetenceopbygning og videnhjemtagning omkring udvikling af AI-teknikker til opdagelse af angreb (intrusion detection) på OT-netværk og IoT-netværk. Dette bygger videre på et nuværende projekt mellem Alexandra Instituttet og Aalborg Universitet. Viden omkring cybersikkerhed vil blive kombineret med viden omkring kunstig intelligens. Vi vil udbygge vores samarbejde med vidensinstitutioner gennem en F&I ansøgning.

[1] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[2] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

	Der vil blive lavet en afdækning af nuværende og kommende krav indenfor sikring af kritisk infrastruktur og kritiske systemer. Denne afdækning vil bruges til at målrette aktiviteter i dette aktivitetsområde i denne periode, og kommende perioder, samt indgå som en vigtig del af vidensprednin indenfor dette aktivitetsområde. Der vil formentligt blive gennemført en eller flere cases i samarbejde med aktivitetsområdet omkring standarder og certificeringer. Arbejdet vil bygge på tværfaglige processer, der undersøger teknologiske, brugermæssige, samfundsmæssige og forretningsmæssige aspekter af aktiviteterne og behovene. På baggrund af dette arbejde vil vi udvikle teknologiske services målrettet danske virksomheders behov. Disse services forventes først klart til markedet i en efterfølgende aktivitetsperiode.
3. Aktører *Hvem* udfører aktiviteterne? Hvilken afdeling af instituttet? Evt. hvilke eksterne parter er med (videninstitutioner, virksomheder, erhvervsorganisationer, myndigheder, klyngeorganisationer eller andre).	Direkte involverede GTS Institutter: • Alexandra Instituttet A/S: Security Lab, People Technology and Business Lab og Artificial Intelligence and Data Analysis Lab. Eksterne parter: • Innovationsnetværkene MADE, CenSec og DigitalLead • Erhvervsstyrelsen/CFCS – i forbindelse med EU's cybersikkerhedsforordning • Erhvervsorganisationerne DI og DE • Aalborg Universitet, som vi har et nuværende samarbejde med omkring "Intrusion Detection". Dette samarbejde vil vi forsøge at udvide.
4. Sammenhæng med andre projekter (evt.) Indgår aktiviteten i andre eksternt finansierede projekter?	Denne aktivitet har sammenhæng med RK-indsatsområdet: Digitale teknologier til datadrevet, bæredygtig vækst (Alexandra Instituttet) Eksternt finansierede projekter: • CIDI: Cyber secure IoT in Danish Industry (Industriens Fond). Projektet har til formål at støtte danske IoT producenter med cybersikkerheden i produkterne- • Sb3D: Security by Design in Digital Denmark (Industriens Fond). Projektet har til formal at øge brugen af Security by Design i IT-løsninger produceret i Danmark. • HoneyPot projekt (CFCS). Projektet slutter ved udgangen af 2020, men har givet vigtig baggrundsviden indenfor HoneyPots, som kan benyttes til at sikre OT- og IoT-systemer. • Nyt projekt - Der vil i dette projekt være afsat midler til en ansøgning indenfor området.
5. Følgegruppe Har følgegruppen forholdt sig til aktiviteten? I så fald hvordan? Hvis ikke, hvornår forventes følgegruppen at blive præsenteret for aktiviteten? (Det sidste bør kun gælde under opstarten af indsatsområdet).	Samarbejdet med følgegruppen i denne aktivitet sker gennem løbende involvering af en undergruppe af interessenter gennem aktivitetsområdet *Demonstration af anvendelighed og værdiskabelse ift. indsatsområdet Digital sikkerhed, tillid og dataetik*, hvor risikostyring omkring potentiel konkurrence også vil blive håndteret. Aktiviteten bidrager med faglig viden og forslag på teknologiske services, som følgegruppen orienteres om og efterfølgende forholder sig til.
6. Formidling af resultater (evt). Hvordan/hvor kan interesserede virksomheder og andre få viden om resultaterne af aktiviteterne? (Anføres/tilføjes hvis det ikke allerede fremgår af beskrivelsen ovenfor, f.eks. ved links til konferencer, hjemmeside, publikationer etc.).	Formidling af aktiviteternes resultater vil ske gennem aktivitetsbeskrivelsen *Demonstration af anvendelighed og værdiskabelse ift. indsatsområdet Digital sikkerhed, tillid og dataetik*, hvor denne aktivitet bidrager med fagligt indhold, oversigt over krav, casebeskrivelser, teknologioversigt og demonstration etc. De udviklede ydelser vil også stilles til rådighed for markedet gennem den digitale TDU. OPDATERING: Væsentlige aktiviteter og resultater opnået i 2021: • 2 nye forskningsprojekter: CRUCIAL og SIoT omkring sikring af IoT og OT

	• Kompetenceopbygning omkring NIS og NIS2 direktiverne • Kompetenceopbygning teknisk sikring af kritisk infrastruktur og OT systemer. • Afdækning af virksomheders udfordring indenfor området –inkl. hos leverandører af teknologi til området • Arbejder med risiko og trusselsmodellering indenfor området.