# Standarder og kritiske systemer

| A. INDLEDENDE OPLYSNINGER | |
|---|---|
| **Aktivitetsområde** | Indsatsområdet Digital sikkerhed, tillid og dataetik |
| **Institut** | Alexandra Instituttet (Lead) og FORCE Technology |
| **Titel**<br>*Dækker indholdet af aktiviteterne* | Standarder og kritiske systemer |
| **Nummerering**<br>*Af beskrivelsen* | 2 |
| **Version** | 1 |
| **Periode**<br>*Forventet start og slut* | 01.01.2024 – 31.12.2024 |
| **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**<br>*Hvorfor?* Hvad er målet for aktiviteterne? Hvordan bidrager de til det overordnede mål for aktivitetsområdet? | Denne aktivitet vil fortsætte Alexandra Instituttets og FORCE Technology's involvering omkring certificering, akkreditering samt standardisering af nye avancerede digitale teknologier for øget cybersikkerhed.<br><br>EU har arbejdet med lovgivning indenfor cybersikkerhed, primært i form af NIS2 direktivet, Radioudstyrs Direktivet (RED) og Cyber Resilience Act (CRA), de senere år og de overordnede rammer forventes endeligt vedtaget omkring udgangen af 2023. Virksomheder kan imidlertid endnu ikke begynde implementeringen af disse lovgivninger, da en række detaljer skal nærmere beskrives i harmoniserede standarder (RED / CRA). Implementering er også afhængig af NIS2 udrulning på national plan.<br><br>Hvor de relevante virksomheder og offentligheden som helhed efterhånden er blevet bekendt med eksistensen af NIS2 og de overordnede krav heri, er CRA og RED stadigt relativt ukendte i mange virksomheder. Dette udgør særligt et problem i forhold til CRA, idet lovgivningen også omfatter rene software løsninger. Det betyder at software branchen, som langt hen ad vejen normalt ikke er underlagt regulatoriske krav, ikke kun skal opfylde en række krav i forbindelse med cybersikkerhed, men også skal kunne dokumentere at kravene er opfyldte og leve op til en række andre krav omkring CE-mærkning.<br><br>I relation til både NIS2, RED og CRA, spiller forskellige sikkerhedsstandarder og rammeværk en vigtig rolle, idet de både beskriver hvordan sikkerhedstiltag skal implementeres og også anvendes i forbindelse med kommunikation til eksterne parter.<br><br>Standarder og lovgivning resulterer ofte i en række tekniske tiltag der skal implementeres. For at sikre en reel forbedring af sikkerheden, er man dog også nødt til at overveje hvordan de menneskelige brugere agerer. Aktivitetsområdet vil derfor også undersøge hvordan brugernes opførsels og den dertilhørende kultur påvirker den samlede sikkerhed og hvordan dette kan adresseres. |

| | |
|---|---|
| | Konkret vil aktivitetsområdet have et primært fokus på hvordan virksomheder kan anvende standarder i praksis, hvorved de kan dokumentere deres implementerede sikkerhed. Ydermere, vil aktivitetsområdet, som en af konsekvenserne ved CRA, have et fokus på hvordan software virksomheder kan/skal arbejde med dokumentation i forbindelse med CE-mærkning af deres løsninger.<br>Dette vil opnås gennem virksomhedscases, hvor virksomheder bl.a. hjælpes med at udvikle den nødvendige dokumentation således forskellige, almene sikkerhedsfunktioner kan valideres ud fra en dertil udviklet testplan.<br><br>De udviklede værktøjer, processer og erfaringer vil være tilgængelig i vores TDU-Cybersikkerhed, samt danne grundlaget for aktivitetens videnspredningsaktiviteter. |
| **2. Indhold**<br>*Hvad* skal der ske? Hvilke(n) konkret(e) aktiviteter udføres? | Aktiviteten vil fortsætte med standardiseringsarbejdet fra de tidligere år. Arbejdet foregår i standardiseringsudvalg i Dansk Standard, i EU-regi (f.eks. CEN/CELEC) og internationalt (f.eks. ISO), gennem S-441 udvalget, både som bidrag til og overvågning af relevant standarder. Det aktive arbejde vil primært foregå i arbejdsgrupperne relateret til RED og CRA, dvs. JTC 13 WG9 og SRAHG CRA.<br><br>Udover standardiseringsarbejdet, vil vi også være involveret i lovgivningsarbejdet og fortsat deltage som eksperter, på vegne af DI, i Orgalims taskforce, der giver EU kommissionen input i forbindelse med udarbejdelsen af Cyber Resilience Act (CRA), da lovgivningsarbejdet nærmer sig sin afslutning, forventes aktiviteten i Orgalims taskforce dog at falde. Denne aktivitet bidrager med viden om CRA og giver os mulighed for at dele den nyeste viden om lovgivningsabejdet gennem TDU-Cybersikkerhed.<br><br>Selvom standarderne tilstræber at være forståelige, er de ofte omfattende og komplekse og kan være et uoverskueligt område for virksomheder, særligt hvis virksomheden ikke kan afse tilstrækkelige ressourcer til området. For at hjælpe virksomheder med at komme i gang med arbejdet omkring validering af deres sikkerhedsfunktioner vil der blive udviklet en række eksempler på fremgangsmåder og dokumentationsformer for hvordan dette kan opnås. Her er der fokus på hvordan men kommer fra kravspecifikation til en testet, valideret og dokumenteret funktion. Som nævnt tidligere, vil en række EU love stille krav til virksomhedernes cybersikkerhed i den kommende tid, men samtidigt har virksomhederne relativt kort tid til at implementerede de nødvendige tiltag.<br>Konkret drejer det sig om RED med effekt fra August 2025, mens de beskrivende harmoniserede standarder der skal implementeres, tidligst bliver færdigarbejdet i løbet af 2024. Noget tilsvarende gælder CRA, som forventes at få en indkøringsperiode på 2 eller 3 år, men hvor skabelsen af de relevante harmoniserede standarder kommer til at bruge en stor del af den tid. I vores TDU-Cybersikkerhed vil vi lancere en vejledning til, hvordan virksomheder bliver berørt af den nye lovgivning, og hvordan virksomhederne allerede nu kan begynde på arbejdet omkring compliance. Et særligt fokusområde er i den forbindelse software virksomheder og hvordan de kan arbejde med CE-mærkning.<br><br>Hvis virksomhedernes arbejde med at efterleve de nye krav skal medføre en højere reel sikkerhed, er det afgørende, at det ikke blot behandles som et spørgsmål om compliance, men også om kultur. Det er afgørende at forme medarbejdernes daglige arbejdsgange – men det er også vanskeligt. Som supplement til vores materialer om compliance vil vi derfor udvikle et workshopformat med tilhørende materialer, som skal understøtte virksomhederne i at udmønte deres sikkerhedspolitikker på en måde, som medarbejderne kan forstå og efterleve. Vi vil tilbyde facilitering af en sådan workshop gennem vores TDU-Cybersikkerhed.<br><br>En anden udfordring, som aktiviteten vil adressere, handler om hvordan små og mindre virksomheder kan overholde NIS2, Større virksomheder vil ofte vælge at implementere ISO 27001 og derved opfylde kravene, men ISO 27001 er omfattende og |

| | |
|---|---|
| | kan hurtigt være for stor en opgave for små virksomheder. I den forbindelse vil aktiviteten kigge på hvordan mindre og lettere rammeværk, som f.eks. D-mærket, kan anvendes til at sikre at kravene i NIS2 er opfyldt i mindre virksomheder.<br><br>Aktiviteten vil derudover adressere de særlige krav og udfordringer der findes indenfor kritisk infrastruktur. Det arbejde ligger i forlængelse i de eksisterende projekter Crucial og CyPro, der fokuserer på hhv. overvågning af kritisk infrastruktur og cybersikkerhed i produktionsvirksomheder.<br>Aktiviteten forventes ligeledes at have synergi med sporet "Data & AI governance", idet opsamling af data til beskyttelse af (kritiske) systemer i sig selv kan indebære en risiko, der kan mitigeres ved brug af teknikker beskrevet i "Data & AI governance" sporet.<br><br>For at sikre virksomhederneds efterlevelse og kompliance med relevante krav indefor cybersikkerhed, skal arbejdet omkring akkreditering jf ETSI EN 303 645 og ETSI TS 103 701 færddigøres, hvilken forventes at være afsluttet Q2 2024. Resultatet heraf vil være, at virksomheder kan tilbydes en uvildig gennemgang af deres produkter med tilhørende inspektionsrapport og certifikat jf den/de standarder, der er omfattet af akkrediteringen. Akkrediteringen og servicen forventes efterfølgende udbygget, så den kan understøtte de kommende standarder i forbindelse med CRA og RED. Dette gøres tilgængeligt via TDU-Cybersikkrhed.<br><br>Vi vil så vidt muligt aligne diverse guides med D-mærket og sikkerdigital.dk, således processer og dokumentation kan genbruges hvor muligt. |
| **3. Aktører**<br>*Hvem* udfører aktiviteterne? Hvilken afdeling af instituttet? Evt. hvilke eksterne parter er med (videninstitutioner, virksomheder, erhvervsorganisationer, myndigheder, klyngeorganisationer eller andre). | Direkte involverede GTS Institutter:<br>• Alexandra Instituttet A/S: Security Lab, Insights Lab, Artificial Intelligence and Data Analysis Lab samt Strategic Business & Governance dept.<br>• FORCE Technology Product Compliance.<br>• Samarbejde gennem Nordic IoT Center.<br>Eksterne samarbejdspartnere:<br>• Dansk Standard<br>• Klyngerne MADE, CenSec og DigitalLead<br>• D-Mærket<br>• DIGST<br>• Erhvervsorganisationerne DI og DE<br>• Universiteter, vi allerede har samarbejder med: AAU, DTU, ITU og AU<br>• Orgalim – Europe's Technology Industries |
| **4. Sammenhæng med andre projekter (evt.)**<br>Indgår aktiviteten i andre eksternt finansierede projekter? | RK-indsatsen medfinansierer og sikrer sammenhæng til følgende igangværende projekter:<br>• Crucial (Grand Solution): I projektet skal Alexandra instituttet, Aalborg Universitet, Ørsted og Grundfos i tæt samarbejde udvikle og teste algoritmer, der kan beskytte kritisk infrastruktur.<br>• AI-Matters, TEF (Digital Europe): Formålet er at udvikle en europæisk testplatform, hvor fremstillingsvirksomheder kan teste sine AI teknologier.<br>• European Digital Innovation Hubs: TechCircle (CD-EDIH/Midtjylland), SE-DIH (Sydjylland), AI Boost (GC-EDIH/Hovedstaden)<br><br>Ovenstående projekter leverer 1) behovsafdækning, udvikling, modning og pilottest af relevante TDU services i RK-indsatsen som er under udvikling og 2) relevant videnspredning til målgruppen.<br><br>Øvrige projekter, der bl.a. bidrager med viden og adgang til RK indsatsens målgruppe: |

| | |
|---|---|
| | • CyPro: CyberSikker Produktion i Danmark, Industriens Fond: Projektets formål er at styrke cybersikkerheden indenfor IoT i Danske produktionsvirksomheder – både producenter og aftagere af IoT.<br>• Sb3D: Security by Design in Digital Denmark, Industriens Fond: Projektets formål er at øge brugen af Security by Design i digitale produkter og løsninger.<br>• SIOT: Secure Internet of Things – Risk analysis in design and operation (Innovationsfonden DIREC) projektets formål er værktøjer til risikoanalyser indenfor cybersikkerhed. |
| **5. Følgegruppe**<br>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). | Vi har haft en løbende dialog med repræsentanter fra Dansk Standard, EnergiNet, Hounö, Digitaliseringsstyrelsen, Censec, Eurisco. Den kontinuerlige dialog har muliggjort udveksling af indsigt og erfaring inden for områderne standardisering og kritiske systemer. Udover løbende dialog er der d. 21. november 2023 afholdt møde med følgegegruppen, hvor aktiviteten og delaktiviteterne blev præsenteret og diskuteret. Aktivitetsbeskrivelsen er efterfølgende blevet tilpasset på baggrund af følgegruppens kommentarer. |
| **6. Formidling af resultater (evt).**<br>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.). | Resultater og erfaringer fra denne aktivitet vil primært blive formidlet gennem aktiviteten 'Demonstration af anvendelighed og værdiskabelse' inden for indsatsområdet Digital sikkerhed, tillid og dataetik.<br><br>Formidlingen laves gennem forskellige formater såsom white papers, blogindlæg samt præsentationer på konferencer og webinarer. Desuden vil materialer være tilgængeligt gennem TDU-Cybersikkerhed på alexandra.dk.<br><br>For at nå ud til en bredere målgruppe vil en betydelig del af formidlingen foregå i samarbejde med andre aktører og samarbejdspartnere. |