# Skema: Ansøgning om resultatkontraktmidler 2019-2020

| **Institut(ter):** | **Aktivitetsplan (titel):** | **Aktivitetsplan nr.: 5** | FoU |
|---|---|---|---|
| Alexandra Instituttet og Dansk Brand- og sikringsteknisk Institut (DBI) | Fremtidens cybersikkerhed<br><br>**Idéforslags titel på bedreinnovation.dk:** Fremtidens cybersikkerhed | | |

**1) Manchettekst (kort resumé)**

It-sikkerhed er fremtidens konkurrenceparameter. Aktivitetsplanen styrker Danmark som foregangsland for cybersikkerhed og privacy, f.eks. med blockchain og kryptologi, og højner sikkerheden i virksomheder gennem fokus på en brugerrettet indsats.

**2) Aktiviteten kort (resumé)**

Denne aktivitetsplan bidrager til udviklingen af Danmark som foregangsland inden for både it-sikkerhed og privacy og skal samtidig sikre, at danske virksomheder får bedre sikkerhed ved at have fokus på brugeradfærd. Ved at fokusere på styrkepositioner inden for digitalisering og forskning kan vi styrke vores position som leverandørland[1] inden for området. Både FORSK2025[2] og regeringens Strategi for Danmarks digitale vækst (2018)[3] nævner direkte it-sikkerhed som konkurrenceparameter for danske virksomheder. Målgruppen er softwareudviklingsvirksomheder, aftagere af it-sikkerhedsteknologier, it-sikkerhedsrådgivningsvirksomheder, virksomheder der vil gøre brug af big data og personlige data samt danske virksomheder bredt.

Aktivitetsplanen vil bidrage til opbygning af kompetencer og ydelser inden for ny teknologi og brugeradfærd på it-sikkerheds- og privacyområdet – f.eks. blockchain og differential privacy. Derudover vil aktivitetsplanen have stort fokus på at bringe opbygget viden om avancerede sikkerhedsteknologier i anvendelse i forskellige domæner som f.eks. healthcare og kunstig intelligens og på at få denne viden omsat til ydelser og værdi hos virksomhederne. Det skal gøre det muligt at arbejde sikkert med big data ved at gøre data tilgængelige, der ikke er det i dag, ikke er lovlige at bruge, uden at de er krypteret, eller som vil medføre for store risici for datalæk. Dermed kan aktiviteten blive en katalysator for vækst i dansk erhvervsliv.

Aktivitetsplanen vil også have fokus på, hvordan man kan bruge personlige data sikkert og privatlivsbevarende på nye måder ved hjælp af avancerede sikkerheds- og privacyteknikker og dermed øge tilliden til virksomhederne. Herunder vil der være fokus på sikkerheden i virksomhedernes opfyldelse af persondataforordningen (GDPR), jf. dataportabiliteten (artikel 20). Ydelserne vil være rådgivning, projektforløb og udvikling af løsninger for eller i samarbejde med virksomheder. Aktivitetsplanen vil endvidere bidrage til, at danske virksomheder får en bedre forståelse for brugersiden af sikkerhed og dermed bliver mere resiliente over for cyberangreb og -læk. Disse mål kan opnås med metoder til adfærdsændring, awareness, cybersikkerhedskultur, brugercentreret design og social engineering-forebyggelse. Ydelserne vil være rådgivning og projektforløb, der skal højne sikkerheden i virksomheder.

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

**Cybertruslen kan sænke den digitale omstilling**

Der er et stort behov for at udvikle ydelser inden for cybersikkerhed (også kaldet it-sikkerhed i dette dokument) og privacy, der kan stilles til rådighed for virksomheder, organisationer og institutioner i Danmark. Center for Cybersikkerhed vurderer, at cybertruslen mod danske myndigheder og private virksomheder generelt er meget høj[4]. Ligeledes lyder det, at risikoen for cyberkriminalitet i sundhedssektoren også er meget høj[5]. Cyberkriminalitet kan have omfangsrige konsekvenser. Et angreb på eksempelvis sundhedssektoren kan have store implikationer for patientsikkerheden. En undersøgelse foretaget af Beredskabsstyrelsen og

[1] https://innovationsfonden.dk/sites/default/files/thefuturemarketforcybersecurityindenmark.pdf
[2] https://ufm.dk/publikationer/2017/filer/forsk2025.pdf
[3] https://www.regeringen.dk/media/4766/strategi-for-danmarks-digitale-vaekst_online.pdf
[4] https://fe-ddis.dk/cfcs/cfcsdocuments/cybertruslen%20mod%20danmark.pdf
[5] https://fe-ddis.dk/cfcs/publikationer/Documents/20180704_Cybertruslen_sundhedssektoren.pdf

Dansk Industri viser også, at cyberkriminalitet er det, danske virksomheder er mest bange for, når de vurderer risikoen for en ny krise[6]. En indsats på området vil derfor være til gavn for dansk erhvervsliv.
Den høje trussel har ikke kun betydning i en it-sikkerhedsmæssig sammenhæng. ATV[7] nævner, at truslen kan gå ud over den digitale omstilling bredt i samfundet, da det må forventes, at myndigheder og virksomheder vil være mere tilbageholdende med investeringer, hvis trusselsbilledet fortsat er meget højt. ATV fremhæver derfor sikkerhedskultur som et område, der bør være stort fokus på. At Danmark netop er blevet udnævnt til verdensmester i offentlig digitalisering[8] aktualiserer kun yderligere behovet for at have sikkerhedsydelser klar til at sikre nuværende og fremtidige digitale services hos danske myndigheder og private virksomheder, så Danmark fortsat er med i front inden for digitalisering. Det gælder også udvikling af teknologier, der sikrer, at personlige data forbliver personlige, samtidig med at de kan deles forsvarligt og privatlivsrespekterende mellem organisationer.

**Adgang til uvildig rådgivning, viden og kompetencer**
Danske SMV'er konkurrerer med store internationale aktører om lettere adgang til data, herunder persondata, samt kompetencer og forskning. Det gælder f.eks. inden for kunstig intelligens, kryptologi og udnyttelse af blockchain-teknologi. Blockchain, der eksplicit er i fokus i FORSK2025[9] og i regeringens Strategi for Danmarks digitale vækst (2018)[10], er et område i rivende udvikling. Danske SMV'er har dog svært ved at få uvildig vejledning med fokus på både de forretningsmæssige, organisatoriske og teknologiske aspekter ved at tage blockchain-teknologi i brug. Det samme vil også gøre sig gældende for andre nye sikkerhedsteknologier som f.eks. post-quantum kryptografi. Som GTS-institutter kan vi understøtte og sikre, at danske SMV'er har mulighed for at realisere potentialet i nye sikkerhedsteknologier, uden at ryge i de faldgruber, der kan være forbundet med at afprøve og implementere meget 'hypede' teknologier. Det kan ofte være et problem for danske virksomheder selv at opnå denne viden, hvilket understøttes af Martin Staal Boesgaard (CEO & Founder, MSB Information Security ApS) på bedreinnovation.dk: *"Vores erfaring er, at udvikling af teknologier og produkter på dette område er så teknologisk avanceret, at det overgår de fleste virksomheders egne kompetencer og kapacitet."*

**Tillidsbaseret dataudveksling på tværs af organisationer**
Brancher der involverer kritisk infrastruktur, og som ligger inde med meget sensitive data, er særligt udsatte for cyberangreb. Det er eksempelvis forsyningsvirksomheder og sundhedssektoren. Samtidig gemmer der sig et stort potentiale i de store datamængder, som disse organisationer skaber. Hvis ikke data håndteres forsvarligt, kan forsøg på at realisere potentialet have store implikationer. Vi vil derfor i denne aktivitetsplan have fokus på, hvordan man kan udnytte forskningsmæssige state-of-the-art teknologier, som endnu ikke er slået igennem i erhvervslivet, som f.eks. secure multi-party computation (SMC eller MPC) og differential privacy, der kan gøre det muligt at foretage tillidsbaseret dataudveksling på tværs af organisationer til gavn for virksomheder, myndigheder og de services, den enkelte borger møder, uden at kompromittere it-sikkerheden og den enkeltes privatliv. Jens Roed Andersen (konsulent, med i flere startups og tidligere CISO i Arla og EnergiNet.dk) skriver på bedreinnovation.dk specifikt om det store potentiale i udnyttelse af secure multi-party computation til at løse samfundsmæssige problemer: *"[SMC] bærer i sig evnen til at kunne løse den p.t. gordiske knude med at sætte data fri uden at gå på kompromis med privatlivets fred og dermed krænke brugere og borgeres tillid til systemet."*

[6] https://www.danskindustri.dk/di-business/arkiv/nyheder/2017/11/virksomheder-er-mest-bange-for-cyberkriminalitet/
[7] https://atv.dk/artikler/analyse/cyberangreb-saetter-danmarks-digitale-omstilling-under-pres
[8] https://www.fm.dk/nyheder/pressemeddelelser/2018/07/dk-verdensmester-i-digitalisering
[9] https://ufm.dk/publikationer/2017/filer/forsk2025.pdf
[10] https://www.regeringen.dk/media/4766/strategi-for-danmarks-digitale-vaekst_online.pdf

**Danske SMV'er skal med på dataøkonomien**
Over de seneste år er der kommet fokus på, hvordan man kan skabe nye løsninger for slutbrugere via adgang til data indsamlet om dem, som derefter kan bruges og kombineres på nye måder, den såkaldte *"personal data economy"*.[11] Denne udvikling er startet med ikrafttrædelsen af persondataforordningen, særligt dataportabilitetsretten. Der mangler dog viden om, hvordan mulighederne omsættes til vækst – både fra et teknisk og et forretningsmæssigt synspunkt. Vi vil i denne aktivitetsplan også have fokus på, hvordan man kan anvende avancerede sikkerheds- og privacyteknikker til at løfte dette nye forretningsområde og stille denne viden til rådighed som ydelser, der kan hjælpe danske SMV'er til at komme med på dataøkonomien, samtidig med at de bevarer deres høje tillid fra kunder. Flere kommentarer på bedreinnovation.dk taler om potentialet i at udnytte personlige data. Bl.a. nævner Michael Lind Mortensen (Senior Consultant i Netcompany A/S og bestyrelsesmedlem i Rådet for Digital Sikkerhed): *"At drage nytte af persondata simultant med, at disses beskyttelse højnes er desuden noget, der vil kunne skabe stor samfundsværdi, idet at det giver leverandører klarere ROIs, uden at kompromittere basale individuelle rettigheder..."*. Det er derfor essentielt at hjælpe danske virksomheder med at sikre, at dette bliver gjort sikkert.

**En højnet sikkerhedsadfærd i danske virksomheder**
Gennem tidligere projektaktiviteter (se afsnit 7) hos både Alexandra Instituttet og DBI har vi erfaret, at menneskers interaktion med teknologier ofte kan være en angrebsflade, der kan skabe udfordringer i forhold til sikkerheden. Det understøttes også af tidligere nævnte ATV-rapport. I denne aktivitetsplan vil vi derfor også have fokus på, hvordan man designer og implementerer sikkerhedsløsninger med brugeren i centrum – hvad enten brugeren er medarbejder i en organisation eller en borger. Vi har som en konsekvens af persondataforordningen set et stigende antal rapporterede datalæk fra danske virksomheder, og en væsentlig del af disse er sket på grund af menneskelige fejl. Vi ønsker derfor konkret at højne sikkerhedsadfærden i danske virksomheder og i et større perspektiv for mennesker generelt. Dette gøres ved at udvikle ydelser, der indeholder en kombination af awareness, adfærdsændring, tekniske løsninger, forståelse for sikkerhedskultur og design af sikre løsninger set fra brugerens vinkel.

**Aktivitetsplanens målgruppe**
Målgruppen for de nye teknologiske serviceydelser skitseret ovenfor er: brugervirksomheder, dvs. aftagere af sikkerhedsteknologier og virksomheder der vil udvikle produkter, hvor god it-sikkerhed er essentiel, samt virksomheder der vil bruge data gjort tilgængelige ved hjælp af avanceret kryptologi eller personlige dataplatforme på en ny måde. Derudover er rådgivervirksomheder, dvs. virksomheder der rådgiver andre virksomheder om it-sikkerhed, også en vigtig del af målgruppen. Sekundært breder målgruppen for aktiviteten sig ud til alle danske virksomheder (med fokus på SMV'er) i forhold til den brugerrettede it-sikkerhed og sikkerhedsprocedurer, da datalæk er noget, der kan ramme alle, hvilket i stigende grad er sket, efter at persondataforordningen trådte i kraft tidligere i år.

Målgruppen er bl.a. inddraget gennem Alexandra Instituttets arbejde med rapporten "The Future Market for Cyber-security in Denmark"[12] hvor vi afholdt workshops med danske virksomheder, som udtrykte deres behov og muligheder inden for it-sikkerhed. Derudover har Alexandra Instituttet og DBI gennem arbejdet i den tidligere resultatkontrakt "Sikkerheds- og privacyværktøjer" løbende fået input, og det står klart, at følgegruppen i projektet har haft store gevinster ud af at få hjælp til, hvilke nye teknologier og trends, de bør kigge på, og hvordan de kommer i gang. I denne aktivitetsplan har vi inddraget den feedback, vi fik fra følgegruppen i det tidligere RK-projekt, men som faldt uden for projektets scope. Med denne aktivitetsplan ønsker vi således at udbygge den platform, vi står på, så danske virksomheder forsat kan komme på forkant med de nyeste teknologier inden for it-sikkerhed.

At der findes et behov for de foreslåede ydelser understøttes af kommentarerne på bedreinnovation.dk. Jakob Illeborg Pagter (CTO i Sepior og medlem af Dansk Industris udvalg for informationssikkerhed) nævner specifikt, at det er problematisk for virksomhederne selv at opnå tilstrækkelig viden: *"[Der] er behov for at få let adgang til viden om moderne sikkerhedsteknologier generelt, således at danske virksomheder kan udvikle deres forretning, uden at krav til it-sikkerhed og privacy kommer på tværs."* Michael Nielsen (Apprestige ApS) nævner også samfundsværdien i at udvikle ydelserne: *"Dette forslag vil øge den danske*

*viden om cybersikkerhed gennem rådgivning samt muliggøre udvikling af centrale sikkerhedsteknologier til samfundet."*

**4) Videnspredning og inddragelse**

I denne aktivitetsplan vil vi etablere en følgegruppe med deltagelse af danske SMVer, større danske virksomheder, offentlige instanser og organisationer. Vi vil tilstræbe at få både brugervirksomheder, konsulenter, leverandører samt offentlige og private organisationer (f.eks. Dansk IT, DI Digital, Rådet for Digital Sikkerhed, Forbrugerrådet og FDIH) repræsenteret. I følgegruppen opnås bl.a. en afklaring af Alexandra Instituttets rolle ift. private rådgivere og leverandører mhp. at optimere synergi og komplementaritet og undgå konkurrenceforvridning. Følgegruppen vil hovedsageligt blive inddraget gennem vores rundbordssamtale-koncept, hvor vi inviterer en udvalgt gruppe (på typisk 15-20 deltagere) til at deltage i en samtale om et relevant emne inden for aktivitetens rammer. Det kunne f.eks. være et oplæg om en teknologi, hvor vi har screenet området eller har lavet en løsning. Ud over en diskussion om det givne emne, vil rundbordssamtalerne også være det forum, hvor følgegruppen bliver inddraget i, hvilke emner de synes, de mangler viden om, og som vi derfor kan undersøge. Rundbordssamtalerne bygger videre på det koncept, vi udviklede i resultatkontrakten "Sikkerheds- og privacyværktøjer", da det viste sig, at det var den bedste måde at få aktiveret følgegruppen. Vi vil bygge videre på følgegruppen fra førnævnte projekt, og vi vil løbende invitere deltagere til gruppen inden for den nævnte målgruppe. Ambitionerne er at have en følgegruppe på 40 virksomheder/myndigheder/organisationer i slutningen af 2019 og 50 i 2020.
Ud over følgegruppen vil vi i denne aktivitet løbende udarbejde mindst 8 publikationer af forskellig art, typisk i form af whitepapers der deles med følgegruppen, men også som artikler distribueret i fagpressen som f.eks. Version2 eller Computerworld. Vi vil også tilstræbe at komme ud i fagpressen inden for ikke it-relaterede felter, hvor sikkerhed er en udfordring – noget vi har haft succes med tidligere. Yderligere vil vi tilstræbe at udgive forskningsartikler baseret på den viden, vi erhverver gennem denne aktivitetsplan og relaterede forskningsprojekter.

Der vil også blive sat tid af til at medfinansiere afholdelse af et sommerkursus i Identitet og Privacy på kandidatniveau på Aarhus Universitet, hvor nye teknologier og viden inden for området bliver tilrettelagt kandidatstudenterende i datalogi for dermed at sikre, at den nyeste viden på området kan blive overført til virksomhederne. Der vil også være et øget fokus på at være involveret i kandidatprojekter på alle universiteter i Danmark.

I aktivitetsplanen vil der også blive etableret et samarbejde med flere af innovationsnetværkene, deriblandt InfinIT og Inno-Sec. Arbejdet med innovationsnetværkene fungerer godt i dag, og i fremtiden ser vi det styrket gennem et fokus på følgegrupper og fælles aktiviteter som f.eks. workshops og rundbordssamtaler. Resultatet af disse samarbejder kan også bruges til at føde ind i, hvilke teknologier der bør kigges på i aktiviteten. Ud over dette vil netværkene blive brugt til at dele relevante resultater fra projektet for at nå ud til flere virksomheder.

**5) Konkrete aktiviteter**

Denne aktivitetsplan er både teknisk og brugerorienteret, og aktiviteterne afspejler dette. Vi vil i aktivitetsplanen arbejde ud fra følgende metode til at udvikle ydelser og opnå kompetencer:

1. Afdækning af behov.
2. Udvikling af kompetencer/ydelser.
3. Afprøvning og demonstration.
4. Videnspredning.

I alle faser af aktivitetsplanen vil vi så vidt muligt søge feedback fra følgegruppen og innovations-netværkene. Det konkrete arbejde er organiseret inden for fem kategorier som beskrevet i det følgende.

[11] https://mobileecosystemforum.com/wp-content/uploads/2016/11/Understanding-the-Personal-Data-Economy-Whitepaper.pdf

[12] https://innovationsfonden.dk/sites/default/files/thefuturemarketforcybersecurityindenmark.pdf

**Kompetencer**
Denne kategori har fokus på at udvikle/videreudvikle de nødvendige kompetencer i Alexandra Instituttet og DBI. Arbejdet her vil være baseret på de behov, der afdækkes i de andre kategorier i dette afsnit. Arbejdet vil bestå af desktop research af state-of-the-art, deltagelse i relevante konferencer og netværksmøder, skrivning af videnskabelige artikler, skrivning af forskningsansøgninger og – i relevant omfang – certificeringer. Disse kompetenceopbyggende aktiviteter vil blive omsat til viden, der kan bruges under de andre kategorier og i et relevant omfang blive omsat til whitepapers. Målet med aktiviteterne inden for denne kategori er at opbygge viden, der er nødvendig/central i de øvrige kategorier, og som kan føre til konsulentydelser, der mangler på markedet i dag. Følgende liste viser de kompetencer, vi vil opbygge, som derefter kan omsættes til konsulentydelser:

- Brugeradfærd inden for sikkerhed og privacy (analyse af brugeradfærd, brugeradfærdsændring, f.eks. awareness-tools, design af brugervenlige sikkerhedsløsninger/processer, design af adfærdsændring).
- Kryptografi (forskellige former for avanceret kryptografi inkl. post-quantum kryptografi, dvs. kryptografi der er fremtidssikret imod angreb, hvor der bruges kvantecomputere).
- Blockchain-teknologier og implementeringer.
- Privatlivsfremmende teknologier (Privacy Enhancing Technologies, PET's), f.eks. machine learning-baserede privacy-assistenter, og løsninger baseret på avanceret kryptografi.
- Sikker big data-analyse som giver adgang til brug af data, der i dag ellers ikke ville være muligt (f.eks. beregning på krypteret data gennem MPC og avanceret anonymisering som f.eks. differential privacy).
- Domæneviden om sikkerhed og privacy i forhold til nye trends og megatrends som f.eks. differential privacy og blockchain.

**Metoder og værktøjer**
Her er der fokus på at udvikle metoder med det formål, at de kan leveres som en ydelse til de virksomheder/organisationer, der har behovet. Vi vil i denne kategori hovedsageligt arbejde med to ting: Mål 1) er at udvikle metoder til at arbejde sikkert og privatlivsbevarende med big data og personlige data, for at muliggøre adgang til data, der er utilgængelige i dag. Det kan f.eks. være på grund af lovgivning, der umuliggør datadeling, eller fordi de personlige data er låst til en enkelt leverandør, hvilket der med blandt andet dataportabilitetskravet fra persondataforordningen nu skal åbnes op for. Mål 2) er at udvikle metoder til at lave en samlet brugerrettet indsats for at højne sikkerheden i danske virksomheder. Dette sker gennem en kombination af test af organisationers modstandskraft/resiliens mod cyberangreb via social engineering og andre angrebsvektorer samt en brugercentreret analyse af medarbejdernes arbejdsgange samt metoder til kultur- og adfærdsændring. I 1) vil fokus være på at finde en metode til at anvende avancerede sikkerheds- og privacyteknologier til at arbejde med big data og det personlige data space. I 2) vil der være fokus på at udvikle metoder til at forbedre den medarbejderrettede sikkerhed i virksomheder, herunder et specifikt fokus på at kunne levere ydelser af forskelligt omfang, som kan komme alle SMVer til gode og ikke kun dem med store budgetter. Der vil derfor være fokus på at levere ydelsen i tre forskellige størrelser, så alle virksomheder kan få gavn af arbejdet. Følgende liste indeholder eksempler på de metoder, vi vil opbygge gennem aktiviteten:

- Konkrete metoder til arbejde med big data på en sikker og privatlivsbevarende måde.
- Metoder til ændring af sikkerhedsadfærd.
- Metoder til awareness.
- Metoder til fokus på brugersikkerhed.
- Metoder til brugercentreret design af sikkerhedsløsninger.

**Screeninger**
I denne kategori skal der arbejdes bredt med at screene forskellige områder af sikkerhed og privacy. Det kan være i form af anvendelse af en teknologi, implementeringer af teknologi på markedet, screeninger af brugeradfærd, screening af et antal virksomheders anvendelse af en teknologi. Outputtet af en screening kan være enten en publikation i form af et whitepaper, input til en løsning eller input til, hvad der er brug

for i metodeudvikling eller kompetenceopbygning. Nedenstående liste er eksempler på, hvad en screening kunne være:

- Post-quantum kryptografi, konkrete implementationer.
- Blockchain-teknologier og blockchain-baserede løsninger.
- Sikkerhedsadfærd i virksomheder.
- Brugercentrerede designmetoder for sikkerhed og privacy.
- Awareness-værktøjer.
- Anvendelser af personlige data med fokus på sikkerhed og privacy.

**Innovative løsninger og ydelser**

På baggrund af screeninger og metodeopbygning skal der under denne kategori arbejdes med at udvikle løsninger og helt konkrete ydelser. Disse vil også være baseret på feedback om behov fra følgegruppen. Vi forventer, at disse løsninger vil udfylde huller i viden og værktøjer hos danske virksomheder. I udviklingen af ydelser og løsninger vil vi anvende brugerinddragelse og workshops. De udviklede løsninger vil have form af metoder, teknikker og software, der tilbydes virksomhederne som rådgivningsydelser, softwaremoduler, softwareudviklingsbistand og kortere eller længere projektforløb. Der er i aktivitetsplanen konkrete ydelser, der skal udvikles. Disse er samlede brugerrettede sikkerhedsydelser, som er en kombination af Alexandra Instituttets og DBIs ekspertiser gennem projektforløbet. Nedenstående liste indeholder eksempler på løsninger og ydelser:

- Teknikker til beregning på krypteret data og avancerede anonymiseringsmetoder bruges til at lave løsninger, der ellers ikke ville være mulige, til f.eks. at samkøre data fra sundhedssektoren med andre data, det ikke er muligt at samkøre i dag.
- Løsning hvor brug af personlige data understøttes af avancerede sikkerheds- og privacy-teknikker og dermed gør ting mulige, der ellers ikke ville være det, f.eks. at berige et datasæt under et behandlingsforløb med aktivitetsdata, individerne selv opsamler.
- Blockchain-baseret løsning på et problem, hvor manglende gensidig tillid ellers er en udfordring.

**Vidensprednin og forretningsudvikling**

I denne kategori skal der arbejdes med vidensprednin som beskrevet i afsnit 4. Derudover vil der være fokus på forretningsudvikling for de ydelser, som kommer ud af de øvrige kategorier. Vi vil her arbejde med forretningsudviklingsspecialister i Alexandra Instituttet. Arbejdet i denne kategori bygger på arbejde fra den tidligere resultatkontrakt "Sikkerheds- og privacyværktøjer", hvor vi udviklede en iterativ metode baseret på business model canvas, hvor relevante tekniske specialister arbejdede om at forretningsudvikle ydelser gennem et antal workshops.

Inden for vidensprednin vil vi sørge for at komme så langt ud som muligt. I første omgang vil vi sprede viden til følgegruppen gennem afholdelse af en række følgegruppemøder, da følgegruppen ses som de primære aftagere af projektet. Derudover vil vi skrive et antal artikler til fagpressen inden for it og it-sikkerhed (som beskrevet i afsnit 4). Vi vil også skrive et antal artikler til relateret fagpresse om it-sikkerhed. Det kunne f.eks. være et indlæg i Energibranchens eller Tandlægernes blad. Yderligere vil vi holde oplæg på nationale konferencer om emner fra de andre kategorier i dette projekt. Det kunne f.eks. være et oplæg om resultatet af en screening. Der vil også blive sat midler af til afholdelse af enten en konference eller workshop om et område, der er relevant i forhold til projektet. Det kunne f.eks. være en mere generel konference om de nyeste trends inden for it-sikkerhed eller en workshop med et lidt mere snævert fokus som f.eks. anvendelse af anonymiseringsteknologier i big data. Følgende liste indeholder eksempler på konkrete aktiviteter, der kunne være indeholdt i denne kategori:

- Forretningsudvikling af anvendelse af anonymiseringsteknologier i sundhedssektoren.
- Forretningsudvikling af deling af personlige data på en sikker måde, der ikke er mulig i dag.
- Artikel om screening af quantum kryptografi-implementeringer i Version2.
- Workshop om brug af anonymisering i "the personal data economy".

**Risici og barrierer**
Denne aktivitet er både teknisk og brugerorienteret. Da den tekniske del hovedsageligt er baseret på cutting-edge-teknologier, giver det en stor risiko i forhold til at sikre, at markedet og samfundet efterspørger arbejdet. Dette imødegås ved at kombinere de tekniske sikkerhedseksperters viden med Alexandra Instituttets ekspertiser inden for kravsafdækning og forretningsudvikling. Vi vil blandt andet arbejde med business model canvas[13], casevirksomheder og rundbordssamtaler med følgegruppen, for at få afdækket hvor der måtte være muligheder og behov.
I den brugerorienterende del står det klart, at der er et stort behov for at få fokus på at gøre sikkerheden for medarbejdere større, bl.a. på grund af persondataforordningen og de offentliggjorte datalæk, der er kommet frem i den sammenhæng. Dette – kombineret med at der i fagpressen ofte tales om, at "medarbejderne er den største trussel" – vidner om, at der er behov for at højne sikkerheden i virksomhederne ved at fokusere på medarbejderne. Der findes derfor et behov i markedet, og risici i den brugerorienterede del er derfor mindre (i forhold til at sikre, at markedet og samfundet efterspørger arbejdet).

## 6) Nyhedsværdi og ambitionsniveau

Aktivitetsplanen vil have fokus på at udvikle nye services og ydelser, der er foran markedet, for at højne it-sikkerheden i danske virksomheder med SMVerne som særligt fokusområde. Dette gøres gennem to mål i forhold til ydelser:

**Konsulent- og softwareudviklingsydelser inden for nye sikkerheds- og privacy-teknologier**
Første mål for aktivitetsplanen er at give danske virksomheder nemmere adgang til nye teknologier, ved at vi som GTS-institutter afsøger den nyeste viden inden for it-sikkerhed og privacy og afprøver den i praksis. Dette gør, at virksomhederne ikke behøver investere en masse ressourcer i at afprøve de nyeste trends men i stedet kan opnå viden om disse gennem denne aktivitet. Ydelsen vil dermed bestå i en konsulentydelse i form af rådgivning om nye specifikke it-sikkerheds- og privacy-teknologier og en ydelse, hvor vi tilbyder at udvikle eller hjælpe med at udvikle løsninger med disse teknologier eller projektforløb med virksomhederne. Da der er tale om den nyeste viden og de nyeste teknologier, eksisterer disse ydelser ikke på markedet i dag, og de forventes at kunne udbydes allerede i løbet af projektet og umiddelbart efter.

**Rådgivning om brugerrettet sikkerhed og ydelse om forbedring af sikkerhed i virksomheder**
Det andet mål for aktivitetsplanen er at tilbyde en samlet ydelse inden for en brugerrettet it-sikkerhedsindsats. Der er kommet fokus på, at medarbejderne i virksomhederne har stor betydning for sikkerheden, blandt andet i forhold til udfordringer omkring social engineering. Derudover har Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) udgivet en rapport, hvori agenturet lægger vægt på, at cybersikkerhedskulturen er vigtig for at opnå god sikkerhed i virksomheden[14]. I forbindelse med persondataforordningen er der også kommet fokus på awareness. Nyhedsværdien i denne ydelse er, at vi kombinerer ekspertiser i it-sikkerhed, it-sikkerhedsteknologier og it-sikkerhedsværktøjer med erfaringer fra brugerundersøgelser, brugercenteret design og antropologiske studier fra Alexandra Instituttet og awareness og social engineering fra DBI med henblik på at udvikle en samlet ydelse. Der findes ikke i dag en så omfattende ydelse inden for brugerrettet it-sikkerhed på markedet, som vi som to GTS-institutter samlet vil kunne tilbyde. Ydelserne fra denne del af projektet er rådgivning og konkrete projektforløb med fokus på adfærdsændring, sikkerhedskultur, social engineering, design af processer og awareness-tools samt længere projektforløb baseret på metoder til at højne sikkerheden i virksomhederne.

## 7) Vidensamarbejde og -hjemtagning

Alexandra Instituttet har allerede et tæt samarbejde med Aarhus Universitet inden for it-sikkerhed, og der er også opnået et vist samarbejde med Danmarks Tekniske Universitet, IT-Universitetet i København, Aalborg Universitet og Københavns Universitet gennem tidligere aktiviteter. Det er planen, at denne aktivitetsplan skal skabe et mere permanent samarbejde med disse institutioner inden for it-sikkerhed, blandet andet ved sammen at søge forskningsprojekter. Det er også planen at samarbejde med nationale spillere inden for it-sikkerhed som f.eks. Rådet for Digital Sikkerhed (hvor Alexandra Instituttet er repræsenteret i

[13] https://strategyzer.com/canvas/business-model-canvas
[14] https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

bestyrelsen), Smart city Cybersecurity Lab og OWASP Danmark. Internationalt er det planen at hjemtage viden ved at deltage i konferencer og at samarbejde med internationale partnere gennem forskningsprojekter (især Horizon 2020) og netværk (f.eks. Trust in Digital Life (TDL) og European Cyber Security Organization (ECSO), hvor Alexandra Instituttet er medlem begge steder, samt MyData, hvor Alexandra Instituttet har været med til at starte den danske hub og har været med til at præge organisationen fra starten). Internationalt er der aktuelt et konkret forskningssamarbejde om it-sikkerhed med bl.a. Philips, Technical University of Eindhoven, University of Murcia og IBM Research Zürich. Et Horizon 2020 projekt med Luxembourg Universitet er netop ansøgt.

I forhold til forskningsprojekter vil aktivitetsplanen bygge videre på etableret viden fra en række afsluttede projekter, bl.a. ABC4TRUST (EU FP7) om brugerstyring baseret på avanceret kryptografi (attribute-based credentials), BdBS (Industriens Fond) og PRACTICE (EU FP7) om beregninger på krypteret data (MPC) og DOGANA (EU H2020) og SAVE om social engineering og awareness. Derudover bygger aktiviteten videre på viden fra den nuværende resultatkontrakt "Sikkerheds- og privacyværktøjer", som både Alexandra Instituttet og DBI er/var en del af. Aktiviteten vil også have synergieffekter med flere nuværende forskningsprojekter, bl.a. SODA (EU H2020) om MPC og differential privacy samt brugerstudier af teknologierne, OLYMPUS (EU H2020) om attribute-based credentials med fokus på design til brugere og brug i eksisterende it-løsninger samt HD360 (Innovationsfonden) om brug af data i sundhedssektoren, herunder samtykke, sikkerhed og sikker brug af data. Derudover er der netop sendt en ansøgning om projektet SAFE (EU H2020) om it-sikkerhed generelt med rumindustrien som specifikt domæne. I forhold til forskningsprojekter, planlægges det at skrive nye ansøgninger som en del af denne aktivitetsplan.

Der vil i aktivitetsplanen også være fokus på at styrke den danske indflydelse i OWASP[15], en verdensomspændende non-profit organisation med fokus på forbedring af sikkerhed i software. Fordelen ved at få indflydelse her er, at vi kan rette fokus mod de udfordringer, dansk erhvervsliv står med, og dermed gøres outputtet af OWASPs arbejde mere relevant for danske virksomheder, fremfor at bruge resultater der udspringer af f.eks. det amerikanske marked. Derfor er det naturligt, at vi som GTS-institutter deltager i et sådant arbejde pga. vores viden om udfordringerne i Danmark, som opnås med inddragelse af følgegruppen. Dette udføres ved involvering i at stable den danske afdeling af OWASP på benene.

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

**Alexandra Instituttet A/S**

I Alexandra Instituttet er cybersikkerhed et eksplicit fokusområde i vores strategi og et område, hvor vi har til hensigt at udbygge både F&U-aktiviteter men i særdeleshed også kommercielle services og ydelser rettet mod danske virksomheder. Alexandra Instituttet har spidskompetencer inden for cybersikkerhed, herunder dyb specialiseret viden om avanceret kryptografi, blockchain og anonymiseringsteknologier kombineret med viden om brugerinddragelse og brugervinklen i forhold til sikkerhed og privacy. Der er dog behov for at følge med og vedligeholde denne viden og for bredere specialistviden inden for cybersikkerhedsområdet, da det er et område i rivende udvikling, både hvad trusler og nye teknologiske muligheder angår, og fordi der fra samfundet og dansk erhvervsliv er fokus på, at der er brug for avancerede løsninger og ydelser. Denne aktivitetsplan vil være med til at styrke Alexandra Instituttets viden på området og samtidig sikre, at viden fra Alexandra Instituttets tidligere og nuværende F&U-projekter, herunder EU-projekter, hurtigt kan komme dansk erhvervsliv til gode i form af konkrete ydelser baseret på den nyeste viden inden for feltet. De ydelser der bliver udviklet i dette projekt vil blive forankret i Alexandra Instituttets Security Lab, som i forvejen har ydelser på området. Ydelserne vil blive udviklet på tværs af labs internt, og der er i aktivitetsplanen fokus på at inddrage både forretningsudviklingseksperter og antropologer fra andre labs, samt at relatere og bruge viden og cases til andre domæner, f.eks. healthcare og data science, som i Alexandra Instituttet er labs og fokusområder i sig selv.

[15] https://www.owasp.org/

**Dansk Brand- og sikringsteknisk Institut (DBI)**
Mange virksomheder slås med at opbygge en sikkerhedskultur til at forebygge både brand og forskellige former for kriminalitet. DBI har et strategisk fokus på at opbygge kompetencer inden for adfærdsdesign og awareness. Det har vi bl.a. opbygget via projekter for Forsvarsakademiet og under HORIZON2020. Konkret anvender vi kompetencerne til at hjælpe virksomheder med at forebygge og overvåge angreb med social engineering. Social engineering er cyberangreb, som går målrettet mod vores digitale adfærd. Vores forretningsplan er at omsætte aktivitetsplanen til kommerciel omsætning senest i 2020. Derudover har vi en ambition om at anvende viden om adfærdsdesign og awareness mere generelt, når vi rådgiver virksomheder om, hvordan de skaber en sikkerhedskultur, som forebygger brand og kriminalitet.

**De to GTS-institutter i samarbejde**
De to GTS-institutter har hver især spidskompetencer inden for forskellige dele af cybersikkerhed, kompetencer som komplementerer hinanden rigtigt godt. Et samarbejde om denne aktivitet vil derfor yderligere kunne udbygge samarbejdet og styrke de ydelser, der tilbydes fra GTS-nettet inden for cybersikkerhed, et samfundsmæssigt yderst vigtigt område, hvor GTS bør stå stærkt for at kunne hjælpe dansk erhvervsliv.

## 9) Tidsplan og milepæle

**2019:**
*Vidensamarbejde, -hjemtagning og kompetenceopbygning:*

- 4 publikationer (3 Alexandra Instituttet, 1 DBI)
- 2 forskningsansøgninger. Mindst 1 med en anden dansk videninstitution eller dansk SMV.
- Deltagelse i 2 internationale konferencer.

*Udvikling af teknologisk service:*

- Udvikling af 1 teknologisk løsning der demonstrerer nye sikkerhedsteknologier i en realistisk kontekst, og som kan bruges som grundlag i ydelser.
- Udvikling af 1 brugerrettet sikkerhedsløsning (lille størrelse).
- 3 screeninger.
- Forretningsudvikling for mindst 3 potentielle ydelser.

*Inddragelse og vidensprednin*g:

- Følgegruppe på 25 virksomheder/myndigheder/organisationer.
- Afholdelse af 3 rundbordssamtaler med udvalgte medlemmer af følgegruppen
- Afholdelse af (kandidatniveau) sommerkursus i Identitet og Privacy på Aarhus Universitet.
- 4 artikler i fagpressen.
- Oplæg på mindst 3 nationale konferencer.

**2020:**
*Vidensamarbejde, -hjemtagning og kompetenceopbygning:*

- 4 publikationer (3 Alexandra Instituttet, 1 DBI)
- 2 forskningsansøgninger. Mindst 1 med en anden dansk videninstitution eller dansk SMV.
- Deltagelse i 2 internationale konferencer.

*Udvikling af teknologisk service:*

- Udvikling af 2 teknologiske løsninger der demonstrerer nye sikkerhedsteknologier i en realistisk kontekst, og som kan bruges som grundlag i ydelser.
- 3 screeninger.
- Udvikling af 2 brugerrettede sikkerhedsløsninger (mellem og stor størrelse).
- Forretningsudvikling for mindst 3 potentielle ydelser.

*Inddragelse og vidensprednin*g:

- Følgegruppe på 35 virksomheder/myndigheder/organisationer.
- Afholdelse af 3 rundbordssamtaler med udvalgte medlemmer af følgegruppen

- Afholdelse af (kandidatniveau) sommerkursus i Identitet og Privacy på Aarhus Universitet.
- 4 artikler i fagpressen.
- Oplæg på mindst 3 nationale konferencer.