Sammen mod nye trusler

DANSK ERHVERV

Indhold

DANSK ERHVERV

Juni, 2023

SAMMEN MOD NYE TRUSLER – et ambitiøst dansk cyberpartnerskab

Teknologi og digitalisering er afgørende for lande og virksomheders sikkerhed og konkurrenceevne i en global virkelighed. I Danmark kan vi være stolte af, at vi er et de mest gennemdigitaliserede samfund i verden. Men den øgede digitalisering åbner også nye flanker for kriminelle. Cybertruslen er et grundvilkår. En trussel, der både globalt og mod Danmark er accelereret voldsomt over de senere år med en stigning i antal globale cyberangreb på knap 40 pct. fra 2021 til 2022[1].

Det digitale trusselsbillede forventes ydrligere forværret i de kommende år som følge af tiltagende digitalisering af vores samfund og større tilgængelighed af cybervåben. Det er også reflekteret i regeringens ramme til styrkelse af Forsvaret:

”Cyberspace bliver en vigtigere del af nutidens og fremtidens kampplads og udgør samtidig en høj trussel mod det danske samfund via for eksempel spionage, aktivisme, destruktive angreb og kriminalitet.”
(”Danmarks forsvar og sikkerhed”, regeringen, maj 2023).

Cybertruslen blev meget tydelig i februar 2022, da Ruslands invasion af Ukraine startede med et månedlangt cyberangreb mod landet. Der er ingen tvivl om, at hybridkrig er blevet et fast element af moderne krigsførelse. Det er ikke længere kun geopolitiske magtforskydninger på landkortet og tiltagende spænding i traditionel forstand, der forandrer det sikkerhedspolitiske trusselsbillede. Digitalisering er blevet en så integreret del af vores liv, at både regulære krigshandlinger, terrorisme og organiseret kriminalitet også findes i den digitale sfære. Globalt er EU- og NATO-landene blandt de foretrukne mål.

Samtidig spiller den private sektor en helt ny hovedrolle. Private virksomheder står ofte forrest i skudlinjen – og udvikler og driver samtidig store dele af den kritiske (digitale) infrastruktur. Nationer er afhængige af civilt kontrolleret teknologi i deres forsvar, og en række tech-virksomheder er direkte involveret i krigen i Ukraine.

Et stærkt forsvar mod cyberkriminelle og statsstøttede hackergrupper er derfor blevet en helt essentiel opgave på tværs af militære- og civile aktører og interesser. Modstandsdygtighed er ikke et tilvalg, men en nødvendighed. Det bliver blandt andet tydeligt, når mere end halvdelen af virksomhederne i ’PwC Cybercrime Survey 2022’ har været udsat for et cyberangreb indenfor de seneste 12 måneder.

[1] Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks - Check Point Blog

Vores samfunds sammenhængskraft og fuknktionsdygtighed afhænger af, at de myndigheder, virksomheder og tjenesteudbydere, borgere og virksomheder bruger i dagligdagen, er rustet til at modstå digitale trusler. Der er i den forstand tale om et våbenkapløb, som vi ikke kan undslå os, og hvor vi er nødt til at opbygge kapacitet og samfundsmæssig modstandsdygtighed, så vi sikrer, at cybertruslen ikke bliver en hæmsko for Danmarks sikkerhed og danske virksomheders globale konkurrenceevne.

Sikkerhedspolitik kan – med andre ord - ikke længere adskilles fra digitaliseringspolitik og erhvervspolitik. Moderne trusler går på tværs af både landegrænser og sektorer. Og vores modsvar bliver nødt til at forholde sig til den nye virkelighed.

Regeringens udmeldte ramme for en styrkelse af forsvaret fra maj 2023 sender et vigtigt signal om at styrke den danske cybersikkerhedsindsats. Det byder Dansk Erhverv meget velkomment. Men der er brug for, at de signaler nu følges op af handling. Det kræver investeringer – økonomisk og politisk – og det opfordrer vi til afspejles, når de nærmere indsatsområder skal fastlægges i forsvarsforligsforhandlinger, en ny digitaliseringsstrategi, kvantestrategi, finanslov mv. Et løft af cybersikkerhedsindsatsen er nemlig helt afgørende. Både på nationalt og internationalt plan. Både i forsvaret og civilt. Både offentligt og privat. Og i form af et nyt niveau af ambitiøst samarbejde på tværs af sektorer.

I Dansk Erhverv mener vi, at der er behov for en ny helhedstilgang, hvor vi markant oppriori-terer indsatsen for et fælles cyberforsvar i et langt tættere samarbejde mellem den private og offentlige sektor.

Dansk Erhverv foreslår fem indsatsområder:

1. Gør danske virksomheder robuste
2. Mere samarbejde på tværs af sektorer
3. Større internationalt engagement
4. Investeringer i fremtidens kompetencer
5. Udvikling af ny teknologi og innovation

1. Gør danske virksomheder robuste

Danske virksomheder er under konstant angreb fra cyberkriminelle – og mange af vores virksomheder er i virkeligheden en del af vores ***first line of defense*** i den forstand, at deres kerneforretning er med til at drive samfundets vigtige funktioner. Funktioner, som sikrer, at der er vand i hanen, strøm, internet og madvarer i køledisken. Vores evne til at beskytte vores nation og vores sikkerhedspolitiske målsætninger kræver derfor også erhvervspolitiske løsninger.

Vi har et akut behov for at løfte cybersikkerhedsniveauet på tværs af sektorer. Vores samfunds evne til at modstå cyberangreb er helt afhængigt af, at erhvervslivet får et højt fælles niveau for cybersikkerhed. Det kræver både den rette regulering og et styrket samarbejde mellem virksomheder og myndigheder, ligesom det kræver en indsats fra den private sektor, som kan gøre det mere attraktivt for virksomheder at investere i øget cybersikkerhed. Det gælder ikke mindst for den digitale infrastruktur, hvor rammevilkårene for teleselskaberne til at investere markant i cybersikkerhed skal forbedres.

To af de helt afgørende elementer, som kan være med til at styrke cybersikkerheden i erhvervslivet, er den danske implementering af EU's NIS2-direktiv og et øget optag af D-mærket blandt danske virksomheder.

Det europæiske NIS2-direktiv sætter en højere barre for en lang række sektorer – for nogles vedkommende er der tale om virksomheder, der tidligere ikke har været underlagt krav fra myndighederne i forhold til deres sikkerhedsniveau. De omfattede virksomheder står for manges vedkommende med en stor opgave ift. at leve op til direktivets regler, når det implementeres i dansk lov. Det er en god og nødvendig regulering, hvis vi skal ruste Europa til at kunne modstå cybertrusler, men det kræver en fornuftig og balanceret implementering.

NIS2-Direktivet: direktiv om foranstaltninger til et højt fælles cybersikkerhedsniveau i hele Unionen (NIS2-direktivet) er et fælleseuropæiske regelsæt, som har til formål at højne det generelle sikkerhedsniveau ved bl.a. at indføre regulering vedrørende virksomhedernes informationssikkerhedsforanstaltninger. Direktivet skal derved sætte EU og medlemslandene bedre i stand til at imødegå den stigende cybertrussel.

Danske virksomheder skal have den fornødne adgang til relevant viden og vejledning, så NIS2-direktivet (og anden kommende EU-regulering) kan implementeres rettidigt, effektivt og hensigtsmæssigt i Danmark.

NIS2-direktivet skal være implementeret i dansk lovgivning senest d. 17. oktober 2024. Det betyder, at virksomhederne forventes at efterleve direktivets krav senest d. 18. oktober samme år. Myndighederne har imidlertid først frist for at udarbejde lister over virksomheder omfattet af direktivet et halvt år senere i april 2025. Det er uhensigtsmæssigt og skaber unødig usikkerhed blandt danske virksomheder.

Listen med omfattede virksomheder bør naturligvis foreligge rettidigt og førend lovgivningen træder i kraft, så de omfattede virksomheder kan få tid til at indføre de nødvendige organisatoriske og tekniske foranstaltninger, som er nødvendige for at være ***compliant***.

For at sikre bedst mulige vilkår for virksomhederne, skal direktivet samtidigt harmoniseres på tværs af sektorer og landegrænser, så virksomheder med hovedsæde i Danmark ikke bliver mødt med forskellige krav på tværs af Europa.

Implementering af NIS2-dirketivet kommer for mange virksomheder til at være den primære opgave – uanset om de omfattes direkte eller i andet led som leverandører – og det er ikke det sidste stykke regulering, vi har set fra EU. Fx skal alle produkter med digitale elementer leve op til en række krav, når ***Cyber Resilience Act*** **(CRA)** træder i kraft.

Danske virksomheder har derfor brug for nogle værktøjer, som kan give en ramme for at arbejde struktureret med deres cybersikkerhed. Her er D-mærket et visionært projekt, der har potentiale til at danne skole internationalt. Derudover kan D-mærket være med til at løse en gordisk knude indenfor cybersikkerhed, men som man nu i NIS2-direktivet stiller krav til: sikring af virksomhedens værdikæde.

D-mærket er den første mærkningsordning for digital sikkerhed og ansvarlighed udviklet i et tæt og forpligtende samarbejde mellem Dansk Erhverv, SMV: Danmark, Dansk Industri, Forbrugerrådet TÆNK og Industriens Fond. D-mærket tilbyder virksomheder et konkret værktøj til at arbejde struktureret med deres digitale sikkerhed og ansvarlighed gennem dokumentation og politikker.

Nogle EU-medlemsstater har tilsvarende etableret lignende mærkningsordninger, og det er afgørende, at markedet ikke fragmenteres, så virksomheder skal vælge mellem flere sammenlignelige ordninger, der ikke er harmoniserede. Derfor arbejder vi i Dansk Erhverv for, at D-mærket skal løftes op på europæisk plan og være fundamentet for en fremtidig europæisk mærkningsordning.

D-mærkets udbredelse skal være langt større, og der bør iværksættes et tættere samarbejde herom mellem D-mærkets parter og relevante myndigheder.

Større udbredelse af D-mærket blandt danske virksomheder kræver blandt andet, at mærkningsordningen anerkendes af relevante myndigheder som et middel til at blive *compliant* med minimumskravene i NIS2-direktivet.

Ligesom myndighederne spiller en stor rolle ift. implementering af NIS2-direktivet og udbredelse af D-mærket, kan den offentlige sektor blive en driver for bedre cybersikkerhed i danske virksomheder. Den offentlige sektor indkøber produkter og tjenester for 415 mia. kr. årligt. Leverandører til det offentlige mødes af en række krav både ift. selve leverancen og virksomhederne bag.

Hvis de offentlige indkøbere begynder at stille krav til leverandørernes cybersikkerhed i kvalitetsvurderingen af de virksomheder, der leverer produkter og tjenester, vil det give et stærkt incitament til, at en meget stor gruppe virksomheder får kigget deres cybersikkerhedsforanstaltninger efter i sømmene. I den forbindelse kan D-mærket være en af de måder, som virksomhederne kan bruge til at dokumentere deres cybersikkerhedsniveau overfor de offentlige indkøbere.

Derfor foreslår Dansk Erhverv, at:

- Der nedsættes en hurtigt-arbejdende *task force* med repræsentanter fra myndigheder og erhvervslivet, som senest 1. november 2023 skal udarbejde lister over danske virksomheder omfattet af NIS2-direktivet. I regi af denne *task force* udarbejdes vejledninger, som kan give danske virksomheder den nødvendige viden om, hvordan de kan efterleve direktivets krav til informationssikkerhed – herunder ift. leverandørsikkerhed.

- Der på længere sigt allokeres ressourcer hos sektormyndighederne til at sikre en mere proaktiv og målrettet vejledning til danske virksomheder i forbindelse med implementeringen af ny cyberlovgivning (fx Cyber Resilience Act).

- Der etableres kontakt til vores nabolande og største samhandelspartnere for at sikre maksimal harmonisering med de lande, hvor mange danske virksomheder har aktiviteter, og den danske implementering ikke overimplementerer NIS2-direktivet til skade for danske virksomheders konkurrenceevne.

- De danske myndigheder anerkender D-mærket som dokumentation for virksomheders efterlevelse af minimumskravene i NIS2-direktivet, så snart minimumskravene i direktivet er klarlagt og implementeret i D-mærkets kriterier.

- Cybersikkerhed tages med som parameter for kvalitetsvurdering af virksomheder i forbindelse med offentlige udbud, herunder SKI-rammeaftaler – og D-mærket anerkendes som dokumentation for virksomheders cybersikkerhedsniveau.

- Den danske regering arbejder for, at D-mærket anvendes som model for et mærke på EU-niveau, hvilket kan ske gennem et pilotprojekt for europæisk udbredelse i samarbejde med EU-Kommissionen. Kommissionen har overfor Dansk Erhverv udtrykt betydelig interesse for et sådant pilotprojekt.

- Reguleringen af telesektoren skal tage højde for, at der er brug for markante investeringer i cybersikkerhed i den samfundskritiske digitale infrastruktur.

2. Mere samarbejde på tværs af sektorer

I takt med et stigende trusselsniveau og en bølge af ny regulering fra Bruxelles er der større behov for samarbejde både på tværs af sektorer i den private sektor, ligesom udviklingen stiller nye krav til offentligt-privat samarbejde.

Derfor var det også nedslående læsning, da FN i deres seneste ***Global Cybersecurity Index***-rapport placerede Danmark på en 32.-plads lige under Kasakhstan, netop fordi placeringen især skyldtes parameteret ***'cooperative measures'***. Uanset rapportens nøjagtighed er der gode grunde til at lægge en indsats i at styrke samarbejdet.

Siden etableringen af Center for Cybersikkerhed (CFCS) har der været debat om centerets placeringen indenfor efterretningstjenesten. Debatten har især handlet om, hvilke fordele placeringen giver i forhold til adgangen til efterretningsoplysninger og samarbejde med andre tjenester, og hvad det giver af ulemper at have en national cybersikkerhedsmyndighed, der er omfattet af tavshedspligt og strenge krav til hemmeligholdelse af oplysninger, når samarbejde med den private sektor i stigende grad bliver afgørende.

Debatten er atter aktuel efter offentliggørelsen af en ny analyse af forankringen af CFCS' virksomhedsrettede indsats, som blev besluttet som en del af 'Aftale om et styrket dansk cyberforsvar' (2021), der blev indgået mellem regeringen, Venstre, Dansk Folkeparti, Det Konservative Folkeparti og Liberal Alliance.

Analysen peger på en række udfordringer. Bl.a. vurderer CFCS et behov for yderligere afklaring ift. telesektoren om den organisatoriske opdeling mellem rådgivning og tilsyn i CFCS-regi. Dette med henblik på at skabe klarhed for televirksomhederne over, hvor rådgivnings- og tilsynsopgaverne er forankret. Det byder vi fra Dansk Erhvervs side velkommen.

Samtidig tvivler Dansk Erhverv på at de ændringer, der for nuværende lægges op til i analysen af CFCS, er vidtgående nok. Det er positivt, at evalueringen af CFCS adresserer behovet for vejledning og rådgivning af virksomheder uafhængigt af styrelsens tilsynsopgave, men det er fortsat uafklaret, hvordan dette skal ske i praksis. Det er centralt for virksomhedernes arbejde med cybersikkerhed, at de kan få efterretninger på niveau med den sikkerhedsklassificering, som de har, samt at CFCS's rådgivning af virksomhederne kan foregå i fortrolighed og helt uafhængigt af deres tilsynsopgave.

Når vi kigger til udlandet, er der en række samarbejdsmodeller, som vi kan blive inspireret af. Uanset hvordan vi vælger at organisere og fordele opgaveløsningen, vil der være fordele og ulemper. Det står dog helt klart, at vi har behov for at tage yderligere skridt for at sikre en tættere og mere tidssvarende samarbejdsmodel, og det bør derfor overvejes, hvordan man bedst tager skridt i den retning.

Spørgsmålet om organisering er kun blevet yderligere aktuelt set i lyset af NIS2-direktivet. I forbindelse med implementeringen af direktivet vil op til 18 sektormyndigheder få en central rolle ift. lovimplementering og tilsyn, hvilket stiller store krav til deres mobilisering, ressourcer og kompetencer.

Behovet for styrket offentligt-privat samarbejde gælder også ift. Danmarks beredskab og operative samarbejde ved større hændelser, som går på tværs af sektorer. Her kan der trækkes på erfaringer fra corona-pandemien, hvor private aktører deltog fast i den Nationale Operative Stab (NOST). Tilsvarende kunne der etableres et organ som, med deltagelse af relevante offentlige og private aktører og Forsvaret, kan kaldes sammen med kort varsel for at håndtere større cyberhændelser.

En reorganisering eller fornyelse af de danske cybermyndigheders ansvars- og opgavefordelingen bør derfor samlet set blive mere konkret, så vi kan diskutere konkrete modeller som alternativer til den nuværende modus operandi.

Derfor foreslår Dansk Erhverv, at:

- Der nedsættes en uvildig arbejdsgruppe bestående af repræsentanter fra relevante myndigheder, erhvervslivet, interesseorganisationer og forskere, som skal opstille forskellige mulige modeller for organiseringen af myndighedsopgaver og ansvar, inkl. forslag til styrket offentligt-privat samarbejde. Arbejdsgruppen skal afrapportere senest d. 1. december 2023 med henblik på efterfølgende politisk drøftelse og regeringsbeslutning om fremtidig organisering.

- Der i dialog mellem Center for Cybersikkerhed og telesektoren skabes klarhed om, hvornår centeret agerer som tilsynsmyndighed, og hvornår CFCS varetager sin rolle som rådgiver for virksomheder i den kritiske infrastruktur.

- Der etableres et nyt operativt, koordinerende organ (et digitalt 'War Room'), som kan indkaldes ved større cyberangreb for at sikre koordination og videndeling mellem alle relevante aktører. Forummet mødes derudover to gange årligt for at drøfte beredskabsplanlægning på cyberområdet.

Netop målsætningen om at styrke det offentlig-private samarbejde var også baggrunden for etablering af Cybersikkerhedspagten. Dansk Erhverv bakker op om det hidtidige arbejde men mener, at **Cybersikkerhedspagten skal revitaliseres og styrkes.** Pagten er stiftet af medlemmer fra den offentlige og private sektor i 2022. Siden hen har nye medlemmer ønsket at indgå i pagtens arbejde. Men der er behov for, at flere virksomheder fra industrien – og ikke kun tech-virksomheder – og myndigheder på flere niveauer deltager, hvis pagten skal leve op til sit formål. Derudover kan pagtens arbejde styrkes ved at flere af de operative myndigheder, som har ansvar for cybersikkerheden på deres ressort, optages som medlemmer.

Cybersikkerhedspagten er et offentligt-privat samarbejde, der skal sikre, at danske små- og mellemstore virksomheder (SMV'er) bliver de mest cybersikre i Europa. Gennem en fælles og koordineret indsats skal Cybersikkerhedspagten løfte danske SMV'ers digitale sikkerhedsniveau til det højeste i EU. Samtidig vil pagtens parter arbejde for at gøre danske virksomheders digitale sikkerhedsniveau til en konkurrencefordel. Pagten har det første år arbejdet i tre spor om hhv.:

- **Kompetencer**
- **Varslinger**
- **D-mærket**

De eksisterende tre spor i Cybersikkerhedspagten kan med fordel suppleres, så bl.a. regulering, forskning og innovation inddrages som kernespor i pagtens fremtidige arbejde. Der er en række nye regler på vej i regi af EU – udover NIS2 som nævnt bl.a. ***Cyber Resilience Act*** – og det forventes, at der også de kommende år vil blive stillet forslag til regulering af cybersikkerhedsniveauet.

Derudover ser vi i Dansk Erhverv et behov for at sikre, at Cybersikkerhedspagten i højere grad gøres til et forum, der også tager de svære, dilemmafyldte og strategiske beslutninger op til debat. I øjeblikket har Cybersikkerhedsrådet rollen som rådgiver for regeringen og er også et offentlig-privat samarbejde, men for bedst mulig koordination og brug af de knappe vidensressourcer vil det være en fordel at få samlet alle offentlig-private initiativer, herunder også de initiativer, Cybersikkerhedsrådet pt. håndterer, under Cybersikkerhedspagten. For at understøtte dette bør en ny model for offentlig-privat samarbejde afprøves, hvor også sekretariatsfunktionen etableres, så det spejler medlemssammensætningen.

Derfor foreslår Dansk Erhverv, at:

- Cybersikkerhedspagten revitaliseres og medlemskredsen i pagten udvides til at omfatte flere aktører fra forskellige private sektorer og myndigheder på både kommunalt- og regionsniveau.

- Der etableres to nye spor i Cybersikkerhedspagten indenfor: 1) EU-policy & balanceret regulering, og 2) forskning & innovation.

- Kompetencesporet får større opmærksomhed – fx gennem et samarbejde med det danske Cyberlandshold.

- De eksisterende fora på cybersikkerhedsområdet, såsom Cybersikkerhedsrådet, Cyberpagten mv., tænkes sammen, og at sekretariatsbetjeningen også foregår i et offentlig-privat samarbejde på tværs af myndigheder og organisationer for at sikre transparens i arbejde og et større engagement fra alle parter samt reelle og mere strategiske drøftelser.

3. Større internationalt engagement

Danmark skal have en **stærkere international stemme,** som sikrer, at vi er bannerfører for større EU-harmonisering af regler og styrket europæisk og transatlantisk samarbejde på cyberområdet. Cyberangreb og -kriminalitet er en global udfordring – og forretning – og angreb på danske myndigheder og virksomheder har ofte oprindelse udenfor Danmarks grænser. Samtidig opererer mange danske virksomheder internationalt. Derfor kræver det koordination og samarbejde på tværs af landegrænser for at løse udfordringerne.

I Dansk Erhverv er vi glade for, at der er taget nogle vigtige skridt, som skal sikre Europa mod cyberangreb. Det gælder både ved at stille krav til nogle af de virksomheder, der er afgørende for driften af samfundet, og ved at stille krav til cybersikkerheden i produkter med digitale elementer. Formålet med reguleringen er noget, vi bakker op om, men det stiller store krav til myndighedernes evne og ressourcer til vejledning og tilsyn.

Udover EU-niveauet vil det ikke mindst være afgørende at sikre tættere cybersikkerheds-samarbejde mellem Europa og USA, som både er vores vigtigste sikkerhedspolitiske allierede og største samhandelspartner. Derfor er det også positivt, at der investeres politisk kapital i transatlantisk samarbejde mellem EU og USA på teknologiområdet i regi af Trade & Technology Council, og den højniveau-dialog der finder sted der om nogle af de mest presserende emner på den digitale agenda. Her er cybersikkerhed og samarbejde om at opbygge både defensiv og offensiv cyberkapacitet et oplagt emne, ligesom dialog om regulatorisk harmonisering bør være en prioritet.

Også i regi af NATO er cyber blevet ophøjet til et selvstændigt domæne, og hvor nye teknologier og det digitale trusselsbillede i det hele taget er kommet meget mere i fokus i løbet af de seneste få år. Fx har NATO etableret en innovationsfond, og sidste år blev det besluttet, at et af DIANA[2]-initiativets centre, som fokuserer på dual-use, herunder sikkerhedsmæssige aspekter af kvanteteknologi, bliver placeret ved Niels Bohr Instituttet i København.

Der er et stort behov – og et stort potentiale – for at Danmark engagerer sig endnu mere aktivt på den internationale teknologi- og cybersikkerhedspolitiske agenda.

[2]DIANA: Defence Innovation Accelerator for the North Atlantic

Derfor foreslår Dansk Erhverv, at:

- Danmark taler med en højere stemme på den digitale og cybersikkerhedspolitiske dagsorden internationalt. Det skal bl.a. ske ved, at Danmark sammen med ligesindede EU-lande øger fokus på at sikre en effektiv cyberregulering, der er realistisk for myndighederne at implementere og ikke unødigt overbebyrder virksomhederne. Målet bør også være, at cyberregulering i EU harmoniseres på tværs af alle 27 medlemslande.

- Danmark engagerer sig (endnu) mere aktivt i NATO's 'emerging and disruptive technology'-agenda, inkl. via opbakning og udnyttelse af de nye programmer for privatsektor-involvering og innovation (fx DIANA, 'NATO *Innovation Fund*', 'NATO *Cooperative Cyber Defence Centre of Excellense*' m.v.).

- Styrke medfinansieringspuljen fra de nuværende 38 mio. kr. årligt til 50 mio. kr. årligt, blandt andet for at kunne styrke forskning i cybersikkerhedsløsninger - medfinansieringspuljen tæller med i Danmarks NATO-bidrag.

4. Investeringer i fremtidens kompetencer

Danmark bør satse massivt på **kompetencer indenfor cyber- og informationssikkerhed,** der lige nu er en akut mangelvare hos både virksomheder og myndigheder. På europæiske niveau anslås det, at der er 3,5 mio. ledige stillinger indenfor cybersikkerhed. Og efterspørgslen er støt stigende. Det gælder fx indenfor OT-sikkerhed[3], hvor en række danske virksomheder selv har oprettet et uddannelsesforløb. For at forbedre cybersikkerhedsniveauet er der desuden brug for langt flere medarbejdere med kompetencer indenfor penetrationstest, netværksanalyse, sårbarhedsscanning m.m.

Samtidig opretter flere universiteter målrettede uddannelsesforløb, som kan udklække den næste generation af cybersikkerhedsspecialister. Det giver dog først et afkast på lidt længere sigt, og det kræver, at der skabes interesse i at blive uddannet indenfor cybersikkerhedsområdet blandt de kommende studerende.

Behovet for cyberspecialister er akut, og vi har i Danmark brug for at tænke i en mere holistisk indsats. De regerende europamestre på det danske Cyberlandshold, som i dag er sponsoreret af Industriens Fond, har skabt synlighed og interesse for cyberområdet, samtidig med at indsatsen har givet flere hundrede unge mennesker stærke cybersikkerhedskompetencer.

Derudover har CFCS med Cyberakademiet skabt en god uddannelsesmulighed for personer, for hvem det ikke står lige for at gå den traditionelle uddannelsesvej. Endelig har muligheden for at aftjene sin værnepligt som Cyberværnepligtig været en stor succes – endda så stor, at de unge efter endt værnepligt søger væk fra Forsvaret, fordi virksomhederne står klar med gode jobtilbud.

Derfor foreslår Dansk Erhverv, at:

- Der afsættes midler mhp. at fordoble antallet af uddannelsespladser, der uddanner cyberspecialister på master-niveau over de næste tre år.
- Der afsættes 5 mio. kr. årligt til Cyberlandsholdet – finansieringen kan findes i forsvarsforliget eller på finansloven.
- Optaget på Cyberakademiet øges, så Akademiet kan optage flere egnede kandidater

[3] OT er en forkortelse for *operational technology* dvs. produktionsmaskineri m.v, ligesom IT er en forkortelse for *information technology*

- Beskæftigelses- og efteruddannelsessystemet øger udbuddet af kurser mv., som kan give deltagere kompetencer til at kunne få arbejde indenfor cybersikkerhed.

- At samarbejdet mellem Forsvaret/Forsvarsakademiet og de civile uddannelser indenfor cybersikkerhed styrkes.

5. Udvikling af ny teknologi og innovation

Det digitale våbenkapløb er i høj grad et teknologisk kapløb. Derudover bliver god cybersikkerhed i stigende grad en konkurrencefordel for danske virksomheder. Og nye løsninger til kryptering af data, adgangsstyring og ***malware detection*** mv. Har et stort eksportpotentiale. Derfor skal vi sikre vores samfund mod de nye trusler, og samtidig understøtte fremtidens forretnings- og jobmuligheder, via udvikling af ny teknologi og innovation.

Vi har i Danmark nogle forskningsmæssige styrkepositioner på cyberområdet. Men der er et stort potentiale for at bruge forskningen til at skabe flere innovative løsninger, som både kan forbedre cybersikkerheden hos virksomheder og myndigheder.

Danmark har bl.a. stærke forskningsmiljøer indenfor krypteringsteknologi, og der findes allerede en række virksomheder, som har deres oprindelse i disse miljøer. Derudover er der også behov for dedikeret forskning i cybersikkerhedens organisatoriske discipliner. Men vi skal op i langt højere gear både ift. **forskning og innovation**, hvis vi for alvor skal kunne få andel i det kæmpestore marked for cyberløsninger, der i 2022 havde en værdi på $173.500.000.000.

En udfordring er, at der mangler øremærkede midler til forskningsprojekter inden for cybersikkerhed. Uden dedikerede forskningsmidler risikerer vi både at mangle kompetencerne og løsningerne til at imødegå fremtidens trusler og at gå glip at fremtidens eksporteventyr.

Derudover mangler der i Danmark et dedikeret center eller en platform, som kan undersøge mulighederne for at styrke samarbejde mellem Forsvaret og erhvervslivet med henblik på at udvikle teknologiske løsninger til Forsvaret – herunder cybersikkerhedsprodukter.

Her er der inspiration at hente fra ikke mindst USA og Pentagons *Defence Innovation Unit* (DIU) i Silicon Valley, hvor der fx er blevet udviklet gode, innovative løsninger ved at sende problemstillinger i udbud i stedet for at udsende detaljerede kravspecifikationer. Erfaringerne fra USA viser, at et center af den type kan understøtte et innovativt økosystem, hvor virksomheder kan få inspiration ved at følge udviklingen hos hinanden, ligesom den tætte kontakt til myndigheder og forsvarsenheder giver et bedre indblik i, hvilken type udfordringer og løsninger, som efterspørges af de centrale aktører.

Derfor foreslår Dansk Erhverv, at:

- Der afsættes midler i forskningsreserven målrettet forskning i teknologiske og organisatoriske løsninger, som kan bruges til at forbedre organisationers cybersikkerhed.

- Der etableres konsortier mhp. at søge midler gennem EU-programmet "Digital Europe" til større projekter, hvor forskere og virksomheder sammen udvikler løsninger med udgangspunkt i virksomhedernes behov.

- Forsvaret, sammen med erhvervslivet og universiteterne, laver et træningsforløb, der med inspiration fra lande som eksempelvis Israel, uddanner flere specialister til deltagelse i militære cyberoperationer, og som med disse kompetencer kan bidrage til at udvikle teknologier og etablere start-ups med vækstpotentiale indenfor cybersikkerhed.

- Der etableres et Innovations- og Teknologicenter, som skal bringe Forsvaret og erhvervslivet tættere på hinanden og sikre konkrete samarbejder i forhold til at udvikle innovative og teknologiske løsninger og produkter på bl.a. cyberområdet.

I takt med, at der udvikles **nye teknologier,** finder cyberkriminelle ud af, hvordan disse kan bruges til at kompromittere data og systemer hos virksomheder og myndigheder. Fx er der en forventning om, at kvantecomputere indenfor en årrække vil kunne bryde fx RSA-kryptering, som er et af de mest udbredte systemer til at sikre fortrolige data.

Det er ikke kun et problem i fremtiden, når teknologien er så langt udviklet, at dette kan lade sig gøre i praksis. Mange data, som virksomheder og myndigheder ligger inde med i dag, kan kompromitteres for så at blive dekrypteret om mange år til stor skade – det kan fx dreje sig om statshemmeligheder, patenter eller udviklingsmateriale til nye lægemidler eller andre produkter med lang udviklingstid.

Samtidig har Danmark en særligt god position på kvanteområdet, som bør udnyttes qua en mere ambitiøs satsning på området. Det er der både store sikkerheds- og erhvervspolitiske og eksportmæssige potentialer i.

Derfor foreslår Dansk Erhverv, at:

- Den danske strategi for kvanteteknologi bl.a. får et særskilt og prioriteret fokus på cybersikkerhed.

- Der som led i strategien søsættes en indsats for øget udvikling og anvendelse af *post quantum cryptography* i danske virksomheder og myndigheder.

- En endnu mere ambitiøs dansk satsning på NATO's teknologi-dagsorden og det danske NATO DIANA-center, som foreslået ovenfor, bruges som fundament for et dedikeret fokus på cybersikkerhed.

DANSK ERHVERV
Børsen
1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. + 45 3374 6000

Vi handler på vegne af vores medlemmer

I Dansk Erhverv handler vi hver dag på vegne af 18.000 medlemsvirksomheder og flere end 100 brancheforeninger. Vi er erhvervsorganisation og arbejdsgiverforening for et af verdens mest handlekraftige erhvervsliv.

Vi tilbyder rådgivning inden for medarbejder- og virksomhedsforhold og politisk gennemslagskraft. Vores indsatser bygger på medlemmernes aktive deltagelse i netværk og udvalg.

I Dansk Erhverv arbejder vi hver dag for, at Danmark bliver verdens bedste land at drive virksomhed i. Til gavn for arbejdspladser, velstand og Danmark i fremgang.

Vi arbejder for et Danmark med sammenhængskraft og handlekraft.

DANSK
ERHVERV