Styrk Danmarks digitale sikkerhed

DANSK ERHVERV

www.danskerhverv.dk

Indhold

DANSK ERHVERV
September, 2025

En ny verden

Global usikkerhed og konflikt. Teknologiske kvantespring. Et tiltagende sammenkog af det fysiske og det digitale domæne, der giver os store fordele, men også skaber nye sårbarheder i den kritiske infrastruktur og alle hverdagens gøremål. Det er en udvikling, der berører borgerne fra tidlig morgen til sen aften, når de fx skal betale for dagligvarer i den lokale butik, bestille tid hos lægen, have adgang til vagtplaner på arbejdet, købe togbilletter eller sikre at el-nettet fungerer, så køleskabet kan holde mælken kold. Og virksomheder – store som små – uanset om de driver kritisk infrastruktur eller købmand nede på hjørnet.

Det er blandt de centrale grunde til, at vi skal tage vores digitale sikkerhed meget alvorligt. I en verden, hvor digitalisering og teknologi er integreret i alle aspekter af vores liv, er cybersikkerhed blevet en afgørende faktor for samfundet.

Truslerne i det digitale domæne er ikke begrænset til specifikke sektorer eller til geografiske områder; de er globale og kan ramme enhver person, virksomhed og organisation, uanset størrelse eller branche. Derfor er det nødvendigt med en omfattende og proaktiv tilgang til cybersikkerhed, der skaber de rette forudsætninger for, at danske virksomheder kan operere sikkert og ansvarligt gennem de nye trusler.

HVAD DEFINERER CYBERTRUSLEN MOD DANMARK?

Sårbarhed: Danmark er et af de mest digitaliserede lande i verden og derfor også et af de mest digitalt sårbare. Med flere digitale døre og vinduer, er der flere steder for kriminelle og fjendtlige aktører at trænge ind.

Kapacitet: Den teknologiske udvikling skaber muligheder for cyberkriminelle og statsaktører, der får nye værktøjer / cybervåben via fx AI og kvanteteknologi til at begå cyberangreb.

Motiv: På grund af den stigende geopolitiske usikkerhed er Danmark i stigende grad blevet mål for cyberangreb. Truslen mod både offentlige myndigheder, virksomheder og borgere er voksende, og det understreger behovet for øget årvågenhed og stærke sikkerhedstiltag.

Cybertruslernes voksende omfang og kompleksitet kræver som modsvar en voldsom acceleration af den digitale robusthed – både i den offentlige og private sektor. Det handler ikke blot om at beskytte sig her og nu, men om at udvikle nye teknologiske løsninger i et tempo, der matcher truslernes udvikling. Imidlertid bærer denne nødvendige oprustning også et stort innovationspotentiale med sig: Når vi investerer strategisk i cybersikkerhed, skaber det ikke

kun tryghed, men kan også drive vækst og innovation, nye forretningsmodeller og øvrig specialisering. Der er et potentiale for at gøre danske løsninger til det sikre og dermed nemme valg. Med andre ord er cybersikkerhed ikke kun en udgift, men rummer også en række enorme muligheder for Danmarks konkurrenceevne, og hvor vi kan lade os inspirere af andre lande, der har investeret massivt i både sikkerhed og teknologi.

De typiske cyberangreb bunder i økonomisk kriminalitet. Cyberkriminelle tager fx en virksomheds forretningskritiske data som gidsel og forlanger en stor løsesum for at frigive data.

Men i verdensbilledet anno 2025 er der også statslige aktører, der ønsker at gøre Danmark ondt. Danske virksomheder og organisationer udgør reelt ofte frontlinjen, der oplever cyberangrebene fra fjendtlige aktører. Disse er mestendels, dog ikke udelukkende, lokaliseret i Rusland, Kina, Iran og Nordkorea, jævnfør Center for Cybersikkerheds seneste cybertrusselsvurdering mod Danmark.

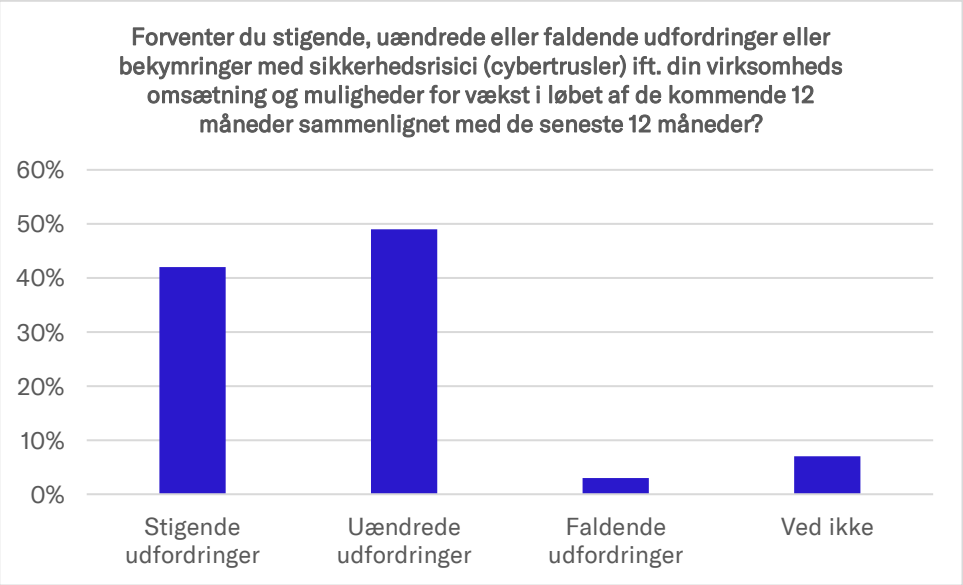
Men er Danmark godt nok rustet til at modstå cybertruslen? Det mener vi bestemt ikke. Vi kan også konstatere, at Dansk Erhvervs medlemmer anser cybertruslen for at være den næststørste udfordring, de står overfor:

Dette udspil har til formål at bidrage konstruktivt til dialogen om Danmarks digitale sikkerhed med fremsynede og konkrete anbefalinger. Cybersikkerhed er en holdsport. Sammen kan vi skabe en modstandsdygtig digital økonomi, hvor frontlinjen mod cybertruslen er overalt, og hvor sikkerhed er nødt til at være en integreret del af den danske digitale infrastruktur. Danmark skal investere langt mere strategisk i cybersikkerhed. For vores sikkerheds skyld – og for konkurrenceevnens skyld.

Cybertruslen er den næststørste udfordring / bekymring for Dansk Erhvervs medlemmer i 2025

36 pct. af Dansk Erhvervs medlemmer har været udfordret eller bekymret ift. sikkerhedsrisici (cybertrusler) det sidste år (75 pct. af virksomheder med 250+ medarbejdere).

42 pct. af Dansk Erhvervs medlemmer forventer stigende udfordringer med sikkerhedsrisici (cybertrusler) det kommende år sammenlignet med det foregående år (54 pct. af virksomheder med 50-249 medarbejdere og 68 pct af virksomheder med 250+ medarbejdere).



Kilde: Dansk Erhvervs medlemsundersøgelse, aug-sep 2024
Note: n = 1.004

Når nedbruddet rammer

God cybersikkerhedspraksis gavner ikke kun erhvervslivet, når danske virksomheder og organisationer udsættes for cyberangreb og nedbrud. Konkrete handleplaner og kommunikationsgange ved nedbrud af enhver type gør, at driften af samfundets kritiske infrastruktur kan fortsætte i perioder med afbrydelser. Investeringer i cybersikkerhed og planer ved nedbrud udgør en fælles forsikring, der styrker samfundets modstandskraft, beskytter borgernes velfærd og hverdag samt sikrer, at Danmark kan opretholde stabilitet og tillid - selv når krisen rammer.

Togtrafikken i Danmark

Den 5. november 2022 blev al togtrafik i Danmark lammet, da et cyberangreb mod DSB's leverandør gjorde lokomotivførernes digitale værktøjer utilgængelige. Hændelsen stoppede togdriften i flere timer, hvilket især illustrerer, hvor afhængige samfundets vitale funktioner er af hele værdikædens sikkerhed – og også SMV'ernes. Mange SMV'er er leverandører til kritisk infrastruktur, men står samtidig over for et komplekst og voksende reguleringslandskab, hvor kravene til cybersikkerhed kan være svære at omsætte i praksis. Uden ressourcer og vejledning risikerer de at drukne i regler frem for at styrke sikkerheden, hvilket kan svække både den nationale forsyningskædes robusthed, befolkningens tryghed – og virksomhedernes evne til at bedrive virksomhed og skabe værdi for samfundet.

Nedbrud på den iberiske halvø

Den 28. april 2025 lammede et strømsvigt Spanien og Portugal og afkoblede den iberiske halvø fra Europas digitale infrastruktur. Hændelsen, der ifølge myndighederne skyldtes teknisk svigt, afslørede, hvor sårbart et moderne samfund er, når kritiske funktioner på tværs af sektorer og lande er tæt forbundne. Et hospital kan have nødstrøm, men det mister hurtigt sin funktion, hvis vandforsyningen svigter, mobilnettet lukker ned, eller leverancer af brændstof til nødgeneratorer ikke kan sikres, fordi kommunikationen er brudt.
Nedbruddet ramte telekommunikation, transport og finans og understregede behovet for tværsektorielle handleplaner, der samler erhvervsliv, myndigheder og forbrugere - nationalt og internationalt. Cybersikkerhed og robust infrastruktur må opbygges som ét samlet forsvar for samfundets funktionsevne.

Styrket internationalt og europæisk samarbejde

Cybersikkerhed er en global udfordring, der kræver en koordineret og fælles indsats på tværs af landegrænser. For at kunne imødegå de komplekse og foranderlige trusler, er det afgørende, at Danmark arbejder for et intensiveret samarbejde i EU, NATO, FN og øvrige internationale institutioner.

Uden et stærkt europæisk og internationalt samarbejde bliver vi ikke i stand til at håndtere cybertruslerne. Og uden et stærkt dansk engagement i dette samarbejde vil vi gå glip af et innovationsniveau, der kan måle sig med resten af verden. Derfor skal Danmark tale med en endnu større stemme og bidrage endnu mere aktivt og konstruktivt på cybersikkerhedsdagsordenen internationalt.

Den voksende mængde digital regulering er, særligt inden for cyber- og datasikkerhed, en måde at sørge for, at vi som samfund løfter i flok. Men den medfører også meget store administrative byrder for europæiske virksomheder og udfordrer deres konkurrenceevne og evne til at trives og vækste i Europa. Derfor er det væsentligt, at Danmark, som et af de mest digitaliserede lande i verden, bidrager aktivt til at forsimple og effektivisere det digitale indre marked. Bl.a. ift. den kommende forenkling af Databeskyttelsesforordningen (GDPR), den kommende revision af Cybersikkerhedsforordningen (Cyber Security Act), samt implementeringer af AI Act, DORA, Cyber Resilience Act og Net- og Informationssikkerhedsdirektivet (NIS2). Det er afgørende for, at virksomhederne kan bruge deres ressourcer mest effektivt på initiativer, der reelt styrker sikkerheden.

Danmark bør desuden stemple endnu mere aktivt ind i det europæiske og internationale samarbejde om fælles standarder og kollektive modsvar mod cyberangreb. I EU ved at styrke cybersanktionsregimet og aktivt bidrage med efterretninger hertil. I Nato ved at bidrage til den fortsatte udvikling og integration af cyberdomænet i kommandostrukturen, tættere cybersamarbejde med den private sektor og flere fælles attribueringer af konkrete cyberanslag. I FN ved at presse på for fremskridt i arbejdet med internationale cybernormer - også selvom det går langsomt, og multilateralismen i FN har trange kår for tiden.

Der er aktuelt betydelig dialog – ikke mindst i EU – om digital suverænitet og behovet for uafhængighed af ikke-europæisk digital infrastruktur, herunder på cybersikkerhedsområdet. I den sammenhæng er det afgørende, at Danmark aktivt engagerer sig i fælleseuropæiske initiativer og bidrager til at forme rammerne for fremtiden. Det imens, man værner om de transatlantiske og andre internationale partnerskaber, som også udgør en vigtig del af vores produktivitet og digitale sikkerhed.

Dansk Erhverv anbefaler

- **Implementering og udvidelse af "Only-once"-princippet**
  Det er essentielt for en effektiv implementering af ny cyberregulering, at både tilsyns- og rapporteringsregimet er simpelt og intuitivt. En fragmenteret implementering af kommende cybersikkerhedsregler i Danmark og på tværs af EU's medlemslande risikerer at skabe unødigt bureaukrati og føre til, at virksomheder underlægges gentagende tilsyn og flere forskellige regelsæt for samme hændelse. Det pålægger erhvervslivet unødige byrder og lægger beslag på ressourcer, der i stedet kunne bruges på at styrke den operative cybersikkerhed. Det er væsentligt, at man i erhvervslivet kan vide sig sikker på, at når man har rapporteret til og lever op til EU-regulering ifølge én myndighed, så accepteres denne compliance på tværs af det indre marked. Derfor anbefaler Dansk Erhverv, at man arbejder efter "Only-once"-princippet både fsva. rapportering og regulatorisk compliance.

- **Etabler et harmoniseret rapporteringsrammeværk på tværs af EU**
  Tilgangen til sikkerhed og data i den digitale lovramme er fragmenteret på tværs af EU, og det ikke kun hæmmer konkurrenceevnen – men også formålet med lovene. Derfor anbefaler Dansk Erhverv, at man går den digitale lovramme efter i sømmene for at skabe en mere simpel og intuitiv tilgang til reguleringen af risici, sikkerhed og databeskyttelse. Særligt for så vidt angår risikovurderinger, hændelsesrapportering og tilsyn, bør man evaluere den akkumulerede mængde af digital regulering som en samlet pakke. Derfor anbefaler Dansk Erhverv, at danske myndigheder arbejder for følgende:

  1. Introduktionen af en tværeuropæisk harmoniseret tærskel for rapportering af væsentlige hændelser, baseret på NIS2.
  2. Fusion af rapporteringstidslinjerne under NIS2 og CRA (samt evt ePrivacy-reglernes sektorspecifikke persondataregler) med GDPR-modellens 72-timer, så man tillader en ordentlig cyberforensisk og analytisk proces inden første rapport, hvilket kan eliminere for hurtige og svært brugbare rapporter.
  3. Et styrket tilsynssamarbejde om hændelsesrapporter, der finder anvendelse under NIS2, CRA, GDPR og anden relevant lovgivning. Hvis man skal rapportere flere gange til flere forskellige myndigheder med forskellige tidslinjer, indhold mm., betyder det, at der på et kritisk tidspunkt tages uforholdsmæssigt meget tid væk fra reel sikring og genopretning af virksomheden selv og dennes kunder, samarbejdspartnere m.v.
  4. Anerkendelsen af NIS2-tilsyn på tværs af grænser. Fragmenteringen af NIS2-implementeringen på tværs af medlemslande skaber væsentlige udfordringer for virksomheder, der opererer på tværs af det indre marked. I flere henseender oplever erhvervslivet således op til 27 forskellige fortolkninger af lovgivningen. Derfor bør man i Danmark og EU arbejde for gensidig

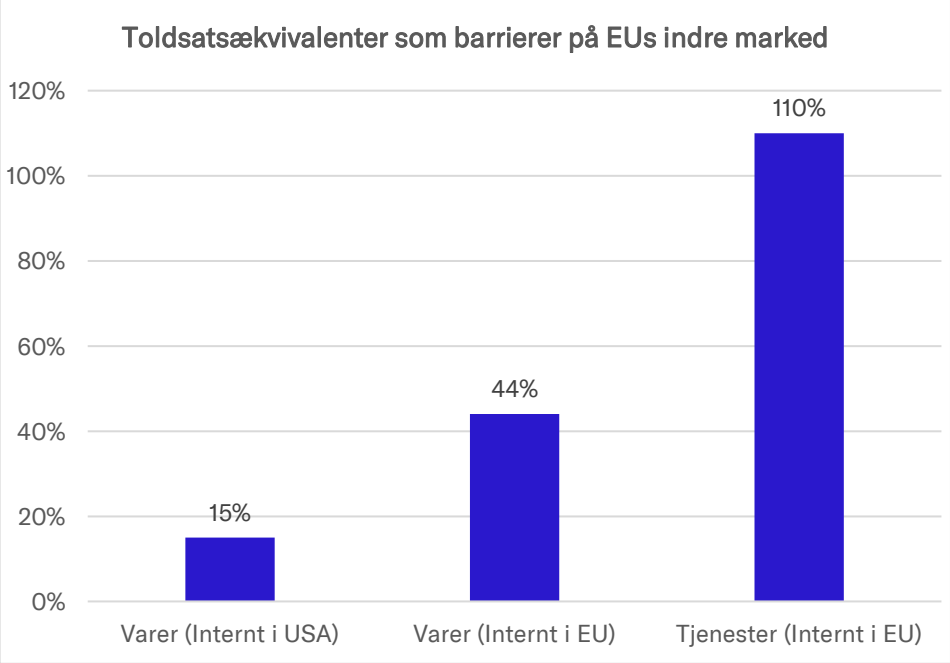
anerkendelse – fx baseret på rammeværk, såsom ISO, CIS18 og D-mærket. I den forbindelse er det vigtigt at implementeringen af NIS2 sikrer balance, og ikke bliver udvandet af laveste fællesnævner. Ligeledes er det i den henseende væsentligt, at en risikobaseret tilgang vedholdes.

5. Udvidelse af cybersikkerhedscertificeringsrammen ifm. revisionen af CSA. Den eksisterende ramme for cybersikkerhedscertificering under CSA er for snæver, da den kun betragter informations- og kommunikationsteknologi (IKT)-produkter, -tjenester og -processer. Dansk Erhverv foreslår, at cybersikkerhedscertificeringsrammen under CSA udvides til også at omfatte virksomheder og organisationer og *compliance*-tjek, så det kan blive lettere for virksomheder at bevise, at de overholder reglerne. Regeringen bør i den anledning arbejde for, at EU-Kommissionen adopterer en dansk tilgang til risikostyring og certificering, eksempelvis ved at løfte D-mærket op på europæisk plan.

Dansk Erhverv er åben overfor dialog om, at NIS2-direktivet kunne omdannes til en forordning og dermed få direkte anvendelse i medlemslandene med øget harmonisering til følge.

EU's barrierer for vækst og sikkerhed

Regulatoriske udfordringer, høje administrative byrder og fragmenterede regler hæmmer den indre samhandel i EU. International Monetary Fund (IMF) vurderer, at de interne handelsbarrierer svarer til en "told" på ca. 44 % for varer og hele 110 % for tjenester i 2020 mod kun 15 % mellem amerikanske delstater[1]. Barriererne varierer på tværs af brancher og skyldes bl.a. dårlig infrastruktur, uens regler og komplekse udbud.



Til sammenligning er EU's eksterne toldsats kun omkring 3 %. Det viser, hvor meget der stadig mangler at blive løftet internt, hvor langt størstedelen af handlen foregår. IMF anslår, at en reduktion af de interne barrierer til amerikansk niveau kan øge EU's produktivitet med op mod 7 procentpoint, hvilket vil halvere det nuværende produktivitetsefterslæb i forhold til USA.

For at opnå det peger IMF bl.a. på følgende indsatsområder:

1. Der skal investeres i infrastruktur på tværs af grænser
2. Regulering skal harmoniseres på tværs af medlemslande

[1]Regional Economic Outlook for Europe, October 2024: A Recovery Short of Europe's Full Potential

Beskyttelse af kritiske sektorer

I kritiske sektorer udbyder både offentlige og private virksomheder produkter og ydelser, der er afgørende for national sikkerhed, økonomisk stabilitet og for danskernes hverdag. Høj cybersikkerhed er således en forudsætning for, at man kan være konkurrencedygtig indenfor blandt andet energi, transport, sundhed, velfærd og finanssektorerne.

Derudover kan et enkelt angreb på en central aktør få kollektive konsekvenser. Derfor skal der tages et kollektivt ansvar.

I takt med, at truslerne mod kritisk infrastruktur intensiveres, bliver modstandsdygtighed på tværs af hele samfundet en strategisk nødvendighed. Derfor er der behov for, at danske virksomheders forudsætninger for at beskytte sig mod cybertrusler styrkes markant. Det gælder ikke mindst de mange SMV'er, der udgør rygraden i både vores økonomi og forsyningskæder og som er enten direkte eller indirekte leverandører til samfundets vitale funktioner og ressourcer. Uden en målrettet indsats for at styrke deres sikkerhedsniveau, svækkes ikke blot virksomhedernes egen konkurrenceevne og driftssikkerhed, men også hele den nationale forsyningskædes robusthed og evne til at modstå koordinerede angreb.

Med ny cybersikkerhedsregulering er kravene til sikkerhed, risikostyring og samarbejde blevet skærpet, og forpligtelsen til at løfte cybersikkerheden er både en national prioritet og et led i en bredere europæisk strategi om resiliens. Det bakker Dansk Erhverv op om. Det er nødvendigt for at sætte en retning i en tid præget af geopolitisk usikkerhed og et meget højt trusselsniveau på cyberområdet.

Nu er det afgørende, at Danmarks digitale modstandsdygtighed styrkes markant. Det betyder bl.a. øget koordinering, samt at den gensidige informationsudveksling om det digitale trusselsbillede mellem myndigheder og private aktører i de kritiske sektorer styrkes. I forlængelse heraf er det vigtigt med et tæt europæisk samarbejde om deling af efterretninger og erfaringer med indsatser og håndtering af hændelser.

Dansk Erhverv anbefaler

- **Styrket samarbejde på tværs af sektorer**
  Forankringen af cybersikkerhed i Ministeriet for Samfundssikkerhed og Beredskab skaber en ny mulighed for at sikre bedre sammenhæng og koordinering af cybersikkerhedsindsatsen på tværs af sektorer. Det handler bl.a. om at samtænke cybersikkerhedsindsatser med det øvrige beredskabsområde herunder særligt

fysisk sikring. De to går hånd i hånd, og derfor er det vigtigt, at cyber- og informationssikkerhed ikke behandles som en isoleret størrelse.

I Danmark er vores krisestyringssystem bygget op om sektoranvarsprincippet. Princippet fungerer langt hen ad vejen til at sikre et effektivt beredskab indenfor de kritiske sektorer, men da sektorerne er tæt forbundne, er der behov for et styrket samarbejde på tværs. Dette bør ikke kun finde sted i tilfælde af en krisehændelse, når den nationale operative stab (NOST'en) træder sammen, men bør være en del af det stående beredskab, så der samarbejdes proaktivt jævnligt på tværs af sektorer. Konkret bør der foretages regelmæssige kriseøvelser med deltagelse af både den offentlige og private sektor.

Forum for bedre NIS2-tilsynsførelse

Den danske model med 10 separate NIS2-myndigheder gør koordination essentiel. Via vidensdeling og samarbejde kan Danmark sikre en bedre implementering af nye cybersikkerhedsregler. Det bør foregå i et forum for tilsynsmyndigheder og NIS2-omfattede virksomheder – fx som et nyt åbent spor i Cybersikkerhedspagten. Dansk Erhverv anbefaler, at Styrelsen for Samfundssikkerhed nedsætter et forum for (til at starte med) NIS2-tilsynsførelse. I den kreds, fx faciliteret af Styrelsen for Samfundssikkerhed, skal erhvervslivet kunne dele erfaringer med tilsynsmyndighederne – særligt mhp. tilsynsmetode og harmonisering. Der er potentiale for i fremtiden også at kunne inddrage bredere rapportering, heriblandt ift. Cyber Resilience Act.

- **Statslig risiko- og sårbarhedsvurdering**

  Der skal hurtigst muligt foretages en statslig risiko- og sårbarhedsvurdering mhp. at afdække sårbarheder og afhængigheder på tværs af kritiske sektorer. Vurderingen skal opstille tværgående scenarier og kortlægge de mest akutte behov for den samlede cyber- og beredskabsindsats. Dette skal som minimum udføres med deltagelse af repræsentanter fra de DORA- og NIS2-omfattede sektorer. Vurderingen kan bruges i tilrettelæggelsen af kriseøvelserne på tværs af sektorer samt til at identificere reguleringsmæssige barrierer for sikring af kritisk infrastruktur.

- **Nationalt cyber 'War Room'**

  Ministeriet for Samfundssikkerhed og Beredskab skal i regi af Erhvervsforum for Samfundssikkerhed og Beredskab etablere et operativt, koordinerende organ (et digitalt 'War Room'), der kan indkaldes ved større cyberangreb for at sikre koordination og videndeling mellem alle relevante aktører. Forummet mødes minimum to gange årligt for at drøfte beredskab på cyberområdet. Dertil er det oplagt, at man i samme forbindelse investerer i regelmæssige kriseøvelser (fx to gange årligt), der inddrager aktører fra yderligere sektorer, da en hændelse sjældent begrænser sig til enkelte områder, men forgrener sig på tværs.

- **Deling af efterretninger**

  Der er brug for bedre videndeling af efterretninger. Derfor anbefaler Dansk Erhverv, at Styrelsen for Samfundssikkerhed arbejder på at skabe et stærkere samarbejde mellem myndighederne og erhvervslivet, der bl.a. vedrører deklassificeringen af efterretninger, så de kan deles med erhvervslivet og navnlig aktører med ansvar for kritisk infrastruktur. Dertil bør myndighederne i højere grad samarbejde med erhvervslivet om udlevering af mere detaljerede og operationelle trusselsvurderinger for SMV'er og alle samfundskritiske sektorer. Dansk Erhverv anbefaler, at Styrelsen for Samfundssikkerhed i samarbejde med private aktører –i regi af Erhvervsforum for Samfundssikkerhed og Beredskab – nedsætter en enhed, der bl.a. skal udarbejde

  1. Kontekstuelle og rettidige 'tekniske' efterretninger, som sikrer, at IT-sikkerhedsmedarbejdere ved, hvad de netop nu skal holde øje med på yder- og indersiden af netværk for at identificere, om der er ubudne gæster. Det kan også være mhp. at reducere usikkerhed ifm. større nedbrud i ind- og udland og dele, hvad myndighederne ved.

  2. Præcise og rettidige 'strategiske' efterretninger, så ledelsen får bedre forudsætninger for at sikre rette prioritering og tildeling af nødvendige ressourcer (jf. DORA og NIS2 krav om ledelsesinvolvering). Eksempelvis bør viden om trusler eller angreb mod konkrete sektorer ideelt deles på forkant på et dybere og mere fortroligt niveau – og i en form, der må deles med ledelsen.

  3. Rapporter om udvikling i trusselsbilledet, heriblandt om specifikke aktørers aktivitet i Danmark og Europa og opbygningen af deres infrastruktur. Her bør man arbejde tæt sammen med bl.a. danske IT-eksperter.

  4. Videndeling fra danske og europæiske cases, hvor man evt. anonymiseret får adgang til beretninger om, hvordan sikkerhedshændelser har udspillet sig, og hvad man kan gøre for at sikre sig selv og samfundet mod lignende hændelser. Det skal fjerne tabuet om at være udsat for cyberangreb og øge modstandsdygtigheden og beredskabet i Danmark.

  Dansk Erhverv anbefaler i den forbindelse, at man lader sig inspirere af den nederlandske Connect2Trust-model, hvor man i et offentligt-privat samarbejde udarbejder (1) deling af sårbarheder/trusler, (2) underretning af berørte, (3) hændelseshåndtering, (4) videndeling, (5) træning/øvelser. (ncsc.nl) Her kan man med fordel involvere cyberleverandørkonsortiet i Security Tech Space.

- **Styrket og tilsynsuafhængig rådgivning til virksomheder**

  Virksomhederne står over for en omfattende opgave med at efterleve de nye

krav og forventninger fra bl.a. NIS2-direktivet og DORA. For at fremme en ensartet og effektiv efterlevelse af de mange nye regler, er det afgørende, at virksomhederne har adgang til specialiseret rådgivning, som er adskilt fra det regulatoriske tilsyn.

I den anledning vil det være hensigtsmæssigt at nedsætte en arbejdsgruppe i regi af Erhvervsforum for Samfundssikkerhed og Beredskab (evt. inspireret af NEKST-modellen fra energisektoren) med repræsentanter fra både den private og offentlige sektor, der skal identificere barrierer og komme med konkrete løsningsforslag til, hvordan det offentlig-private samarbejde kan styrkes herunder, hvordan bedre vidensdeling og tilsynsuafhængig rådgivning kan opnås. I den kontekst anbefaler Dansk Erhverv især, at man øger rådgivningsindsatsen fsva.

1. Vejledning ift. fortolkning af gældende lovgivning.

2. Vejledning ift. ny og kommende lovgivning f.eks. hvad erhvervslivet skal imødekomme af nye lovkrav, herunder kommende lovkrav, såsom Cyber Resilience Act. Lovmedholdighed med en overvældende akkumuleret mængde af regulering på det digitale område er en nødvendig men svær disciplin for danske virksomheder. Derfor bør der tages ekstra skridt for at understøtte især SMV'er ved fx at tilbyde yderligere tilskud til IT-sikkerhedsprojekter.

3. Vejledning ift. leverandørstyring og forsyningskæder, og herunder hvordan erhvervslivet skal forholde sig til brug af leverandører med services fra lande udenfor NATO el. specifikt ift. Kina, Rusland, Iran m.fl. Her bør myndighederne udarbejde risikovurderinger ved indkøb fra specifikke lande, således at den enkelte virksomhed eller fx kommune ikke skal udføre geopolitiske trusselsvurderinger. De nye cybersikkerhedskrav om forsyningskædesikkerhed i NIS2 udgør i øvrigt en væsentlig byrde, da selv små virksomheder har mange leverandører. Tredjepartsleverandører udgør desuden en sårbarhed, hvor et nedbrud kan lamme hele værdikæden - som set i DSB/Supeo-casen. Dansk Erhverv anbefaler derfor nationale vejledninger og standardiserede kontrakttillæg baseret på fx ISO 27036 og ENISA's guidelines, suppleret af støtteværktøjer og en platform til deling af information om kompromitterede leverandører. Det vil reducere fragmentering, øge transparens og understøtte regulatoriske krav.

Styrket cybersikkerhed kræver mindre regulatorisk kompleksitet

Med den danske NIS2-lovs ikrafttræden den 1/7-2025 skærpes kravene til digital sikkerhed i både offentlige og private organisationer. Formålet er at øge modstandsdygtigheden mod cybertrusler og skabe et fælles højt cybersikkerhedsniveau på tværs af erhvervslivet og EU's medlemslande. NIS2-direktivet omfatter 18 sektorer, der er kritiske for samfundets funktion - se direktivets Bilag 1 og 2. NIS2 er vigtigt, fordi det ikke blot stiller krav til tekniske løsninger, men også til ledelsesansvar, rapportering og risikostyring. Det understreger, at cybersikkerhed i stigende grad er et organisatorisk og forretningskritisk anliggende og ikke kun et it-spørgsmål.

Det er både klogt og nødvendigt at fastsætte klare rammer og krav til cybersikkerhed, og ambitioner om at øge opmærksomheden omkring trusselsbilledet samt harmonisering på tværs af erhvervslivet er begge essentielle. Dog risikerer direktivet at have en modsat effekt, da både indhold og krav er meget komplekse, samtidig med at medlemslandenes fortolkninger varierer. Når lovgivning implementeres vidt forskelligt på tværs af EU, bliver virksomhederne ofre for bureaukratiske barrierer, hvorfor omkostningerne ved skalering bliver højere, mens investeringsvilligheden bliver lavere. Det kan åbenlyst skade dansk og europæisk konkurrenceevne, men det er heller ikke godt for cybersikkerheden, hvis vi ikke får en simpel og intuitiv implementeringsmodel for nye cybersikkerhedsregler.

Vi må derfor ikke tro, at cybersikkerhed er en statisk øvelse. Med tiden drager både virksomheder og myndigheder flere erfaringer, som vi bliver nødt til at handle på, tilpasse os og løfte i flok.

De rette kompetencer er fundamentet for et sikkert samfund

For at kunne sikre sin virksomhed, sine kunder og sine samarbejdspartnere, er det væsentligt, at man har de rigtige og kvalificerede kompetencer ansat. Samtidig taler disse kompetencer ind i at løse konkrete samfundsudfordringer i en lang række sektorer. Derfor er det væsentligt, at vi i Danmark adresserer den voksende og uforløste efterspørgsel på kvalificeret arbejdskraft indenfor IT og IT-sikkerhed. Det skal vi via nationale tiltag – men også internationalt, heriblandt navnlig via EU og offentligt-private samarbejde i tråd med *Union of Skills,* EU's strategi for at styrke arbejdsstyrkens færdigheder, opkvalificering og mobilitet på tværs af sektorer, herunder på cybersikkerhedsområdet.

Investeringer i digitale kompetencer er en katalysator for innovation, der ikke kun skaber bedre digital sikkerhed. Det resulterer nemlig i et bredere, længerevarende og mere holistisk udbytte. Diskussionen om forsvarsbudgetterne gør det legitimt, at vi udvikler lokalt og regionalt – og bygger cyberkompetencer i egne brigader. Det er der både arbejdspladser, innovation og sikkerhed i. Men der er også behov for tiltag, der styrker efteruddannelse i konkrete tekniske og faglige kompetencer på it-området og forståelse for, at der er statsaktører og kriminelle i andre lande, der forsøger at gøre skade på Danmark lige nu.

Dansk Erhverv anbefaler

- **Sikkerhedsgodkendelser**

  At ventetiderne for sikkerhedsgodkendelser er en udfordring for særligt IT- og tele- og forsvarssektorerne er veldokumenteret. Ligesom det er et problem for erhvervslivet for at kunne omstille sig organisatorisk og arbejde hurtigt videre med sikkerheden, kan det være en konkurrenceforvridende faktor, at ventetiden på sikkerhedsgodkendelser stiger. Erhvervslivet forstår og accepterer behovet for sikkerhedstiltag som sikkerhedsgodkendelser, og mener derfor, at der må gøres en indsats for at optimere processerne, så sikkerhed og forretningsudvikling kan gå hånd i hånd.

  For at afhjælpe udfordringerne foreslår Dansk Erhverv følgende konkrete tiltag:

  1. Afklaring af krav og forventninger: Der bør være klare retningslinjer og vejledninger for, hvornår det er nødvendigt at opnå en sikkerhedsgodkendelse for at fjerne tvivl og forsinkelser. Der bør endvidere defineres en forventet tidshorisont for sagsbehandlingen af en sikkerhedsgodkendelse, således at virksomhederne ved, hvad de har at forholde sig til, særligt når de byder på

en offentlige opgave. Samtidig er det væsentligt at undersøge, om virksomheder, der potentielt skal kunne løse samfundskritiske opgaver på kort varsel, skal have mulighed for at have sikkerhedsgodkendte personer, uden det nødvendigvis er knyttet til en kontrakt. Virksomheder med fx en rammekontrakt med offentlige myndigheder bør kunne få sikkerhedsgodkendt medarbejdere, selv om de ikke nødvendigvis er knyttet til en nuværende opgave, som kræver godkendelse.

2. Revision af sikkerhedscirkulæret: Sikkerhedsgodkendelser bør gælde på tværs af staten, så medarbejdere ikke skal godkendes flere gange, hvis de arbejder for eller på tværs af forskellige ressortområder – medmindre der i forbindelse med en nye opgave er behov for en godkendelse til et højere klassifikationsniveau.

3. Digitalisering og ensretning af processen: En gennemgribende digitalisering af hele processen fra ansøgning til godkendelse, i en fællesstatslig portal, hvor løsninger som MitID, E-boks, træk fra Skat, CVR, politiets registre og andre relevante registre kan integreres. Dette vil simplificere store dele af processen, minimere procesfejl, forbedre manuelle processer med at indsende dokumentation og give ansøgeren mulighed for at følge med i processen. Tiltaget kan som minimum automatisere mange ansøgninger til "TIL TJENESTEBRUG", hvor bl.a. servicebranchen har mange.

4. En alternativ karensperiode: En undersøgelse af, om myndighederne kan tillade, at virksomheder ifm. ansøgning om sikkerhedsgodkendelse, indsender en dokumenteret baggrundsundersøgelse for at afstedkomme, at den pågældende medarbejder kan få mulighed for at arbejde med dele af sin portefølje, der ikke vedrører sensitive data.

5. Der bør harmoniseres mellem de danske, EU-medlemslandes og NATO's sikkerhedsgodkendelser således, at det er muligt at anvende udenlandsk arbejdskraft og konsulentbistand i de tilfælde, hvor den pågældende medarbejder allerede har en sikkerhedsgodkendelse i et allieret land. Fx ved, at bevis for et andet EU-/NATO-lands sikkerhedsgodkendelse indsendes sammen med ansøgning om dansk godkendelse.

- **Cyberrekrutter: Styrk og udvid den nuværende cyberværnepligt i Fredericia**
  Dansk Erhverv anbefaler, at der foretages en markant styrkelse af de nuværende cybersikkerhedskompetencer. Hvis EU/NATO-lande skal imødegå den voksende cybertrussel samt udnytte sit digitale potentiale, kræver det både flere midler, bedre rammer og mere substans i og omkring eksisterende initiativer. Først må der investeres i at styrke nuværende cyberuddannelser, herunder

cyberværnepligten gennem et længere og mere intensivt uddannelsesforløb samt et højere optag.

Der bør samtidig etableres en cyberkonstabeluddannelse. En specialiseret, praksisnær uddannelse, der kombinerer tekniske færdigheder med operativ erfaring. En sådan uddannelse vil gøre det muligt at fastholde og videreudvikle kompetencerne fra cyberværnepligten og sikre, at vi kan opbygge et varigt og professionelt cyberforsvar. I øvrigt bør man etablere en struktur i Forsvarets reserve til at fastholde cyberværnepligtige efter endt uddannelse.

- **Cyberrekrutter: En ny cyberværnepligt i IT-byen Katrinebjerg**
  Dansk Erhverv anbefaler etableringen af en ny cyberværnepligt. Den nye cyberværnepligt skal bl.a. åbne værnepligten for flere kandidater, der i dag ikke består de fysiske krav, såsom personer med fysisk handicap eller neurodivergente, der også vil bidrage til Danmarks sikkerhed. En ny cyberværnepligt vil styrke Danmarks generelle cyberresiliens – men har også et vækstpotentiale, da værnepligtige kommer ud i erhvervslivet og på de videregående uddannelser fx via Cyber Campus Danmark – se afsnittet '*Investeringer i sikkerhed er ikke et nulsumsspil*'.

  Dansk Erhverv anbefaler, at det undersøges, hvorvidt den nye cyberværnepligt bør forankres i Beredskabsstyrelsen under Ministeriet for Samfundssikkerhed og Beredskab. Placeringen styrker både den nationale cybersikkerhed og samfundets samlede beredskab, samtidig med at den skaber en klar vej fra uddannelse til operativ indsats. Samtidig kan værnepligten i Aarhus kobles direkte til et Cyber Campus Danmark, som har base hos Security Tech Space i IT-byen Katrinebjerg. Det sikrer en klar overgang fra værnepligt til videregående uddannelser, forskning og erhvervsliv – og betyder, at de cyberværnepligtige ikke alene bliver en ressource for staten, men også kan bidrage til nye løsninger, virksomheder og arbejdspladser i erhvervslivet.

- **Større kapacitet af IT- og cybersikkerhedskompetencer**
  Behovet for cyberspecialister og -generalister er akut, og vi har i Danmark brug for at tænke i en mere holistisk indsats. Der bør afsættes midler mhp. at fordoble antallet af uddannelsespladser, der uddanner cyberspecialister på kandidat/masterniveau over de næste år. Samtidig bør Beskæftigelses- og efteruddannelsessystemet øge udbuddet af kurser mv., som kan give deltagere kompetencer til at kunne få arbejde indenfor cybersikkerhed.

  Desværre går udviklingen lige nu den stik modsatte vej. I 2023 vedtog Folketinget en neddimensionering af hele universitetsområdet. Denne såkaldte sektordimensionering sænker optaget, og det er derfor ikke muligt for universiteterne at øge optaget på it-området. Videre vedtog Folketinget i 2021 en udflytning af

uddannelserne fra landets fire største byer. Den aftale betyder, at det ikke er muligt for hverken professionshøjskoler eller erhvervsakademier at optage flere studerende i de fire store byer, hvor både efterspørgsel fra de unge og erhvervslivet er størst.

Dette er to meget alvorlige anslag mod muligheden for at fremme den digitale suverænitet og sikkerheden, da det vanskeliggør opbygningen af yderligere kompetencer på cybersikkerhedsområdet.

Bedre synergier mellem uddannelser indenfor cybersikkerhed

Det er vigtigt at flere kandidater uddanner sig i IT- og cybersikkerhed. Og det er lige så vigtigt, at de samles op efter endt uddannelse. Derfor bør regeringen bl.a. undersøge, hvordan der skabes bedre synergier mellem allerede eksisterende uddannelser. I den henseende er det især relevant at undersøge overgangen fra cyberværnepligt til professionsbachelor i cybersikkerhed, samt overgangen fra professionsbachelor til kandidatuddannelser i cybersikkerhed (som civilingeniøruddannelsen ved Aalborg Universitet). Begrænsningen fremgår af Adgangsbekendtgørelsen (bilag 2), og kan løses ved at give professionsbachelorer adgang, eventuelt med krav om supplerende fag. Denne udvidelse vil styrke talenttilførslen på et af vores samfunds mest kritiske kompetenceområder.

Langsigtet og divers kompetenceopbygning

Selv om flere og flere kvinder i dag læser en it-uddannelse, så er det stadig fortsat først og fremmest mændene, der læser på uddannelserne inden for cyber-området. Fx er kvindeandelen på cyberteknologi på DTU og cybersikkerhed på AAU blot 16 pct. mod godt 30 pct. på it-uddannelserne generelt. Dog er der et lyspunkt på professionsbacheloruddannelsen i cybersikkerhed på Erhvervsakademi København, hvor kvindeandelen er 30 pct.

Hvis vi skal udnytte hele talentmassen, er det afgørende, at det ikke kun er mænd, der arbejder med cybersikkerhed. IT-Universitetet har med stor succes fået flere kvinder ind på it-uddannelserne. Disse erfaringer kunne med fordel udbredes til de øvrige it-uddannelser. Det er samtidig vigtigt at synliggøre, at arbejde med cybersikkerhed ikke kun handler om teknik, men også om kommunikation og projektledelse så fagligt stærke, administrative profiler også ser mulighederne evt. ved jobskifte.

Det er videre vigtigt, at flere både drenge og piger får øjnene op for it-området gennem undervisning om bl.a. digital adfærd, "netetikette" og sikkerhed. Derfor bør digital teknologiforståelse hæves fra et valgfag og gøres til et obligatorisk fag i folkeskolen. Det vil bidrage til, at unge vokser op med nødvendig og grundlæggende cyberhygiejne og –viden, samt øge muligheden for en tidlig interesse herom og deraf potentialet for, at flere vælger cybersikkerhed som karrierevej.

Videregående uddannelser indenfor cybersikkerhed

- Professionsbachelor i Cybersikkerhed v. to erhvervsakademier
- Bachelor i Cyberteknologi v. DTU
- Bachelor i Cyber og computerteknologi v. Aalborg Universitet i København
- Diplomingeniør i Cybersikkerhed v. Aalborg Universitet i København
- Kandidat i Cyber Security v. Aalborg Universitet i København
- Kandidat i Security and Cloud Computing v. DTU i samarbejde med fem nordiske universiteter
- Kandidat i Datalogi med specialisering i cybersikkerhed v. Aarhus Universitet
- Master i Intelligence and Cyber Studies v. Syddansk Universitet

D-mærket: Danmarks – eller Europas? – mærkningsordning for digital ansvarlighed

D-mærket er Danmarks mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse og er stiftet af Industriens Fond i samarbejde med Dansk Erhverv, Dansk Industri, SMVdanmark og Forbrugerrådet Tænk. D-mærket er en uafhængig privat organisation.

D-mærket er sat i verden for at være en hjælp og vejviser for virksomheder, der ønsker at styrke deres digitale ansvarlighed. Mærkningsordningen hjælper virksomheder med at dokumentere, at de arbejder struktureret og seriøst med it-sikkerhed og ansvarlig dataanvendelse og bruges som kvalitetsstempel, der skaber tillid og tryghed blandt kunder, samarbejdspartnere og myndigheder. Samtidig tilpasses D-mærket løbende, og understøtter danske virksomheder i at navigere i og leve op til stigende regulatoriske krav, herunder NIS 2-loven. D-mærket er ikke blot en dokumentation af digital robusthed, men også et redskab til vækst, konkurrenceevne og adgang til nye markeder.

Dansk Erhverv anbefaler, at:

1. Regeringen officielt blåstempler D-mærket, så mærkningsordningen står centralt i regeringens kommende cyberstrategi, og at de danske myndigheder viser, at de anser D-mærket som et konkret værktøj, de har tillid til. Det er afgørende for at få flere virksomheder til at bruge det og dermed højne cybersikkerhedsniveauet.

2. Regeringen anvender D-mærket i sin diplomatiske indsats i EU-regi og i samarbejde med øvrige relevante EU-lande med det mål, at D-mærket danner udgangspunkt for en europæisk mærkningsordning inden for it-sikkerhed og ansvarlig dataanvendelse.

Hvis regeringen for alvor omfavner initiativet og arbejder for en international udbredelse, kan D-mærket blive et internationalt pejlemærke for it-sikkerhed og ansvarlig dataanvendelse. Dermed sender vi et klart signal om, at Danmark ikke kun bruger teknologi, men også er en nation, der sætter standarden for den sikre og ansvarlige digitale fremtid.

Investeringer i sikkerhed er ikke et nulsumsspil

Investeringer i sikkerhed er ikke et nulsumsspil – det kan blive en katalysator for vækst og innovation. Ifølge Niinistö-rapporten fra oktober 2024, *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness*, styrkes Europas konkurrenceevne, udbud af arbejdspladser og innovationsevne, ved at prioritere investeringer i beredskab og kritiske teknologier. Af rapportens analyser fremgår, at én euro i pandemiberedskab under covidkrisen gav en gevinst på 13,3 euro igen, og for hedebølgevarslingssystemer er afkastet op mod 130 euro per euro investeret. Investeringer i forsvarsberedskab, herunder cyber, reducerer risikoen for væbnet konflikt og dermed de ødelæggende sociale og økonomiske konsekvenser, der følger med. At investere i sikkerhed er derfor ikke bare nødvendigt. Det er god økonomisk politik.

Nødvendigheden af investeringer i cybersikkerhed blev yderligere betonet på NATO-topmødet i juni 2025, hvor det blev besluttet, at NATO-medlemslandene fra 2035 årligt skal investere 5% af deres samlede økonomi i forsvar og sikkerhed – herunder 1,5% i bredere sikkerhedsrelaterede anliggender som cybersikkerhed. Med alliancen nye styrkemål er investeringer i cybersikkerhed ikke blot en international forpligtelse, men udgør også en oplagt vækstmulighed for den danske forsvars- og cyberindustri med potentiale for innovation og øget offentligt-privat samarbejde.

Europæiske investeringer mindsker afhængigheden af leverandører i tredjelande og sikrer strategiske sektorer som digital infrastruktur og forsvar. Det øger vores modstandsdygtighed over for kriser og globale forstyrrelser, hvilket både begrænser økonomiske tab og muliggør hurtigere genopretning. Et stærkt europæisk forsvar og sikkerhedsinfrastruktur afskrækker trusler og understøtter langvarig fred og stabilitet i regionen. Samlet set øger de investeringer ikke kun EU's beredskab, men også tilliden blandt borgere og investorer, hvilket er afgørende for Europas erhvervsliv, langsigtede vækst og suverænitet. I øvrigt er det set andre steder på kloden, at innovationsmiljøer i forsvarsområdet også skaber et økosystem af kompetencer, løsnninger m.v., der skaber innovation og succesfulde startupmiljøer i bredere forstand.

Det globale våbenkapløb er i høj grad et teknologisk kapløb. Derudover bliver et tilstrækkeligt niveau af cybersikkerhed i stigende grad en konkurrencefordel for danske virksomheder. Og nye løsninger til kryptering af data, adgangsstyring og malware detection m.v. har et stort vækst- og 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 forskningsmæssige styrkepositioner på cyberområdet. Det medfører et stort potentiale til at bruge forskningen til at skabe flere innovative løsninger, der både kan blive en god forretning og bidrage til vækst og jobskabelse samt forbedre cybersikkerheden hos virksomheder og myndigheder. Det er nødvendigt at skabe rammer, der gør det muligt for virksomheder at skalere, og samtidig styrke forskningsmiljøer, så de kan understøtte scale-ups med viden og kompetencer. Danmark har bl.a. stærke forskningsmiljøer indenfor krypteringsteknologi, og der findes allerede virksomheder, der har deres oprindelse i det miljø. Cybersikkerhed har dog mange facetter, og der er dertil også behov for dedikeret forskning i cybersikkerhedens organisatoriske discipliner, samt på områder som netværkssikkerhed, cyber ed-tech og detektion. Men vi skal op i langt højere gear både ift. forskning, innovation og kommercialiseringsmuligheder, hvis vi for alvor skal udmønte det potentiale.

Dansk Erhverv anbefaler

- **Cyber Campus Danmark – fra trussel til vækst**

  Dansk Erhverv anbefaler, at regeringen investerer i Cyber Campus Danmark med base hos Security Tech Space i IT-byen Katrinebjerg i Aarhus. Cyber Campus skal være Danmarks nationale kraftcenter, hvor forskning, uddannelse, erhvervsliv og offentlige aktører bindes sammen i et partnerskab, der kan vende cybertruslen til et vækstscenarie for Danmark.

  Cyber Campus Danmark skal ikke alene styrke Danmarks forsvar mod cyberangreb, men også skabe grundlag for en ny industri. Investeringer i forskning skal omsættes til innovation, innovation til produkter, og produkter til nye virksomheder og arbejdspladser. På samme måde som Danmark har opbygget styrkepositioner inden for vind og life science, skal cybersikkerhed nu udvikles til et nyt dansk væksterhverv.

  Som en central del af campusset bør der etableres to iværksætterbaser med fokus på cybersikkerhed – én i Aarhus og én i København. Her skal studerende, forskere og startups have adgang til attraktive vilkår, herunder gratis eller reduceret kontorleje, testfaciliteter, inkubatorer og acceleratorprogrammer, hvor det offentlige Danmark og private virksomheder kan fungere som "første kunder". På den måde kan Danmark hurtigt bringe nye løsninger til markedet og skabe eksporteventyr.

  Parallelt med at vi udvider kapaciteten på egne uddannelsesinstitutioner, skal vi i højere grad være i stand til at tiltrække højt specialiseret arbejdskraft fra udlandet – herunder i særdeleshed kompetencer inden for cybersikkerhed. Det vil Cyber Campus Danmark bidrage til, da Danmarks cyberinfrastruktur vil kunne løftes til et niveau svarende til andre Europæiske frontløbere. Fx har Sverige, Estland og Frankrig alle etableret nationale cyber campusser til uddannelse og videndeling.

- **Offentlige udbud som drivkraft for cybersikkerhed**

  Styrkelsen af digital modstandsdygtighed kræver et tæt samarbejde mellem offentlige og private aktører, og dertil et større fokus på og mere ensartet tilgang til cybersikkerhed i offentlige indkøb. I EU køber det offentlige ind for 2000 mia. euro hvert

år, svarende til 14% af EU's samlede BNP. Et stigende europæisk fokus på "joint procurement" såvel som offentlige indkøbs rolle i at sikre europæisk resiliens og EU's strategiske interesser fordrer en øget og strømlinet tilgang til cybersikkerhed. Effekten af en mere strømlinet efterspørgsel fra det offentlige vil derudover være driver for en positiv udvikling både teknologisk og forretningsmæssigt for dansk erhvervsliv. Erfaringer fra fællesinitiativer som Joint Nordic Initiative for Digital Resilience, et samarbejde mellem nordiske myndigheder, brancheorganisationer og techsektorer, viser de mulige gevinster ved koordinering. Initiativet imødekommer et stigende trusselsbillede i Norden samt et mere komplekst regulatorisk landskab, hvor særligt offentlige institutioner og mange SMV'er mangler den nødvendige modstandsdygtighed. Samtidig bidrager det til at undgå et fragmenteret offentligt cyberforsvar, der i dag er en konsekvens af bl.a. offentlige institutioners af varierende tilgange hertil ifm. indkøb. Derfor anbefaler Dansk Erhverv, at der udarbejdes nationale retningslinjer for, hvordan ordregivere indarbejder cybersikkerhedshensyn i offentlige udbud.

I USA har Pentagons Defence Innovation Unit i Silicon Valley vist, hvordan man kan skabe innovative løsninger ved at udbyde problemstillinger i stedet for at lave detaljerede krav. Netop den type (funktions-)udbud bør man fremme af hensyn til at styrke et teknologisk økosystem, hvor virksomheder inspirerer hinanden og får bedre indsigt i de behov, som myndigheder og forsvar efterspørger.

- **Kvanteteknologi og kryptering**

  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.

  Derfor anbefaler Dansk Erhverv, at regeringen gør en særskilt indsats for øget udvikling og anvendelse af post quantum cryptography i danske virksomheder og myndigheder. Investeringer i den type teknologi vil falde særdeles gavnligt, da EU netop er i færd med at investere massivt i European Quantum Communication Infrastructure (EuroQCI) – et paneuropæisk netværk, der skal etablere ultrasikker kvantekommunikation via både jordbaserede fibernet og satellitter. EuroQCI vil danne rygraden i Europas kvanteinternet og sikre, at følsom kommunikation inden for stat, forsvar og kritisk infrastruktur beskyttes mod nye cybertrusler via quantum key distribution (QKD) og avancerede kryptografiske teknologier. Initiativet er allerede i en fremskreden implementeringsfase, og fuld operationel kapacitet forventes i 2027.

DANSK ERHVERV
Børsgade 4
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