Cyberangreb kommer aldrig belejligt

DI's cybersikkerhedsudspil

Dansk Industri

Indhold

1. Offentligt-privat samarbejde om nationale værn mod cyberangreb 10

Forslag 1: Platform for deling af trusselsinformation

Forslag 2: Indføring af et nationalt cyberfilter på internettrafik for at forhindre cyberangreb

Forslag 3: Opprioritering af forskning og innovation inden for cybersikkerhed

Forslag 4: Tværgående cyberberedskabsøvelser

Forslag 5: Cyberberedskabsordning i tilfælde af større cyberangreb

Tema: Teknologi, sikkerhed og konkurrenceevne i en ny geopolitisk virkelighed

2. Cybersikkerhedsløsninger til SMV'er 20

Forslag 6: Enhed for SMV'ers cybersikkerhed – styrket overblik, målrettet vejledning og genvej til handling
Forslag 7: Styrket offentligt-privat samarbejde om udviklingen af D-mærket

3. Uddannelse og cyberkompetencer 24

Forslag 8: Uddan flere IT- og cybersikkerhedseksperter

Forslag 9: Styrket fokus på cybersikkerhed på tværs af universitetsuddannelserne

4. Stærk national sikkerhedskultur 26

Forslag 10: Målret den offentlige oplysningsindsats, så den når ud til borgere og virksomheder

Forslag 11: Public service-institutionerne skal lave mere indhold om digital sikkerhed

Tema: International indsats for styrket cybersikkerhed

Cybertruslen mod Danmark er stigende

Danmark er et af de mest digitaliserede lande i verden. Det har i mange år kommet borgere til gode f.eks. ved nemmere kommunikation med det offentlige, ligesom danske virksomheder har høstet store produktivitets- og konkurrencefordele som følge af digitalisering. Den høje grad af digitalisering betyder dog samtidig en øget sårbarhed over for cyberangreb.

De geopolitiske spændinger sætter et solidt aftryk på den digitale verden, og over de seneste år er truslen fra cyberangreb taget til både nationalt og internationalt. Stater anvender særligt cyberangreb, cyberspionage og cyberaktivisme for at opnå politiske mål, mens ikke-statslige cyberkriminelle særligt har fokus på at opnå et økonomisk afkast f.eks. ved at gennemføre ransomware-angreb.

Særligt russiske cyberangreb mod både virksomheder og offentlige myndigheder er tiltagende, og der ses en stadig større risikovillighed, også i angreb rettet mod Danmark. Moderne våbenkapløb udspiller sig i dag i cyberspace og foregår i gråzonen mellem krig og fred.

Sikkerheds- og beredskabsdagsordenen er et fælles anliggende på tværs af det offentlige og private. Kun med en stærk indsats fra alle fronter får vi styrket Danmarks samlede modstandsdygtighed over for et foranderligt og mere alvorligt trusselsbillede.

Knap 30 pct. af virksomhederne

peger på hybride trusler som den største usikkerhedsfaktor i deres forretning i de kommende år.

Kilde: DI's virksomhedspanel, december 2024

Truslen fra cyberspionage er meget høj

Truslen fra cyberkriminalitet er meget høj

Truslen fra cyberaktivisme er høj

Truslen fra destruktive cyberangreb er middel

Kilde: Cybertruslen mod Danmark, Center for Cybersikkerhed, september 2024

Mere end 50 pct. af danskerne

synes ikke, at vi beskytter os tilstrækkeligt mod hybride trusler, som f.eks. cyberangreb.

Kilde: DI's befolkningspanel, marts 2025

Cybersikkerhed er afgørende for virksomheders forretning og konkurrencekraft

Hver dag bliver danske virksomheder ramt af cyberangreb. Det er derfor ikke længere et spørgsmål om man bliver angrebet, men hvornår og hvor hårdt.

Mange cyberangreb har allerede haft alvorlige konsekvenser for danske virksomheder. Produktionsstop, lammede systemer og tab af data har forstyrret den daglige drift og virksomheders langsigtede forretning med store økonomiske tab til følge. I yderste konsekvens har virksomheder været nødsaget til at dreje nøglen om som følge af cyberangreb.

Samtidig viser undersøgelser som Cyberbarometeret, at cybersikkerhed er et konkurrenceparameter for virksomheder, der investerer i sikkerhedstiltag og dermed gør deres forretning mere modstandsdygtig over for cybertrusler. I fremtiden vil cybersikkerhed og dataetik blive endnu vigtigere konkurrenceparametre for danske og europæiske virksomheder.

Selvom flere og flere virksomheder har fået øjnene op for vigtigheden af at investere i cybersikkerhed, er der behov for et markant løft af sikkerhedsniveauet på tværs af hele erhvervslivet for at imødegå truslernes alvor og omskiftelighed.

38 pct. af store danske virksomheder og 17 pct. af små danske virksomheder har været udsat for cyberangreb de seneste fem år.

Det koster mindst 200.000 kr. per dag, hvis en stor dansk virksomhed rammes af et hackerangreb, hvor it-systemer lukkes ned.

For små virksomheder vil de daglige omkostninger ligge på omkring 47.000 kr. pr. dag.

Kilde: TDC Erhvervs indsigtsrapport 2025

Dette udspil er Dansk Industris forslag til centrale elementer i den nye nationale strategi for cyber- og informationssikkerhed, som skal forhandles politisk i 2025.

Med udspillets 11 konkrete initiativer styrker vi ikke alene cybersikkerheden på tværs af det danske erhvervsliv, men tager også afgørende skridt i retning af at styrke samfundets samlede modstandsdygtighed i en digitaliseret verden.

Det skal ske gennem et stærkt offentligt-privat samarbejde om at:

1. Indføre nationale værn mod cyberangreb og styrke cyberberedskabet
2. Øge cybersikkerheden i SMV'erne
3. Styrke den nationale sikkerhedskultur
4. Fremme cyberkompetencer gennem uddannelse
5. Styrke dansk engagement i internationale cybersikkerhedsindsatser i EU og NATO

Udspillet er en del af en serie af udspil fra Dansk Industri, der sætter fokus på styrkelsen af samfundssikkerheden og beredskabet. Det første udspil satte fokus på erhvervslivet rolle i beredskabet og udkom i december 2024. Dette cybersikkerhedsudspil er andet udspil i rækken og vil følges op af et tredje udspil, som vil fokusere på kritisk infrastruktur.

Strategisk Beredskabsforum bygger bro mellem erhvervslivet og det politiske system

DI har taget initiativ til Strategisk Beredskabsforum, der består af topledere fra udvalgte virksomheder, der alle har ekspertise og viden inden for forskellige sektorer.

Strategisk Beredskabsforum udvikler og kvalificerer politiske anbefalinger sammen med DI med det formål at styrke den samlede nationale beredskabsindsats, så Danmark i langt højere grad er forberedt på at håndtere de trusler, som vi står over for i dag.

Medlemmerne i Strategisk Beredskabsforum er:

- Søren Krogh Knudsen, CEO, Columbus
- Flemming Jensen, administrerende direktør, DSB
- Thomas Egebo, CEO, Energinet
- Jakob Riis, President and Group CEO, Falck
- Troels Bjerg, CEO Asia Pacific/Americas/Germany & Global Business Performance, ISS
- Christian Poulsen, CEO, Københavns Lufthavne
- Caroline Pontoppidan, Chief Corporate Affairs Officer, Mærsk
- Claus Fibiger, CEO, Securitas
- Michael Holm, arbejdende formand for bestyrelsen og tidligere CEO, Systematic
- John Henriksen, CEO, TDC Erhverv

Foruden dette forum har DI's Udvalg for Informationssikkerhed løbende fokus på at komme med input til politiske initiativer specifikt på cyber- og informationssikkerhedsområdet.

DI-medlemmer kan styrke deres forretning med beredskabsværktøjer

Det er vigtigt, at man som virksomhed kender sin forretnings sårbarheder og de risici, der kan sætte virksomheden under pres i tilfælde af krise.

Med DI's risiko- og sårbarhedsanalyser som værktøj kan man få overblik over risici og sårbarheder, vurdere sin modstandsdygtighed, afdække løsninger og initiativer samt prioritere risiko- og sårbarhedsreducerende tiltag.

Med rettidig og grundig beredskabsplanlægning kan man minimere konsekvenserne og komme sikkert igennem i tilfælde af en hændelse. Det kan være alt fra et cyberangreb, en oversvømmelse, energimangel, forsyningskædebrud eller andre kritiske hændelser. DI's skabelon til en beredskabsplan kan bruges til at sikre, at der er styr på kriseledelse, krisestyring, krisekommunikation og kontinuitetsplaner mv., hvis krisen skulle ramme.

Værktøjerne er udviklet i samarbejde med Beredskabsstyrelsen.

D-mærket guider virksomheder igennem de vigtigste standarder inden for it-sikkerhed og ansvarlig dataanvendelse og hjælper virksomheder med at styrke deres digitale modstandsdygtighed.

Som medlem af DI kan man endvidere tilmelde sig DI's følgegruppe for beredskab og løbende modtage relevant information om sikkerhed og beredskab, opdateret vejledningsmateriale og tilbud om at deltage i arrangementer, kurser og webinarer.

Læs mere på **di.dk/beredskab**

1. Offentligt-privat samarbejde om nationale værn mod cyberangreb

Vores nationale værn mod cyberangreb skal op i gear, hvis vi som samfund skal kunne følge med et hastigt foranderligt trusselsbillede, hvor innovative kræfter hele tiden finder nye metoder til at udnytte vores sårbarheder. Det kalder på en flerstrenget tilgang med en stærk indsats på tværs af myndigheder, virksomheder og civilsamfund.

For det første er der et stort uforløst potentiale i at øge videndelingen om trusselsinformation mellem myndigheder og virksomheder for at styrke samfundets samlede modstandsdygtighed og forhindre cyberangreb i at sprede sig.

Både på virksomheds- og myndighedsniveau er vi alt for langsomme til at reagere på truslerne. Det skyldes først og fremmest, at overblikket over angrebsteknikker i dag er fragmenteret. Dels bringes myndighedernes viden ikke nok i spil til gavn for virksomhederne – typisk fordi informationen kommer for sent og er for svær at handle på. Dels er det ofte virksomhederne, der opdager nye hændelser først, og derfor er det afgørende, at erhvervslivet også i højere grad deler information på tværs, hvis vi skal kunne følge med udviklingen.

For det andet er der et stort uudnyttet potentiale i at udbrede eksisterende tekniske løsninger og modne mere avancerede løsninger som værn mod cyberangreb i realtid. Mange løsninger giver gode muligheder for at detektere og blokere cyberangreb og er allerede tilgængelige i dag uden at blive brugt på et systematisk, samfundsmæssigt plan i Danmark. For eksempel er DNS-filtrering en effektiv metode til at beskytte borgere, virksomheder og myndigheder mod cyberangreb såsom phishing, malware og ransomware.

For det tredje er der behov for en opprioritering af forskning og innovation inden for mere sofistikerede cybertrusler, der følger af den teknologiske udvikling.

NIS2-direktivet

har til formål at skabe et højt og ensartet cybersikkerhedsniveau på tværs af EU. NIS2 repræsenterer den mest vidtgående regulering af cybersikkerhed for danske virksomheder og offentlige myndigheder til dato. Direktivet har fokus på beskyttelsen af kritisk infrastruktur og stiller en lang række både tekniske, organisatoriske og ledelsesmæssige krav til cybersikkerhed, herunder krav om basal cyberhygiejne, forsyningskædesikkerhed og hændelsesrapportering.

Implementeringen af direktivet er ét skridt på vejen til at øge samfundets robusthed overfor cyberangreb og beskytte vores kritiske infrastruktur, men det kan ikke stå alene.

Fakta:

- Ministeriet for Samfundssikkerhed og Beredskab forventer, at ca. 3255 virksomheder er direkte omfattet af NIS2 fordelt på 18 sektorer. Dertil kommer en lang række underleverandører, som vil blive indirekte omfattet.
- De erhvervsøkonomiske konsekvenser estimeres til 4,4 – 5,7 mia. kr. i omstillingsomkostninger og 2,7 – 3,8 mia. kr. årligt i løbende udgifter.
- Foruden virksomheder omfattes også statslige myndigheder, kommuner og regioner af NIS2.
- NIS2 træder i kraft i dansk lovgivning den 1. juli 2025. På energiområdet er NIS2-kravene allerede trådt i kraft.

Det gælder ikke mindst automatiserede cyberangreb og kvantecomputere, der kan bryde eksisterende kryptering.

Endelig skal vi styrke vores nationale cyberberedskab, så vi bliver langt bedre til at håndtere cyberangreb, når uheldet er ude. Det kræver først og fremmest gode beredskabsplaner, der løbende testes, og klarhed om, hvem der gør hvad i nødssituationer.

Forslag 1: Platform for deling af trusselsinformation

For at udnytte potentialet i deling af trusselsinformation mellem myndigheder og virksomheder, skal der etableres en platform, hvor viden om aktuelle angreb og sårbarheder kan deles sikkert og fortroligt. Det kalder ikke alene på en teknisk løsning, men også på en kulturændring i retning af større åbenhed og samarbejdsvillighed. Det gælder både for myndighederne, men også i erhvervslivet, hvor det er afgørende, at viden om angreb og udviklinger i angrebsmetoder i højere grad bliver delt, så vi sammen kan undgå, at cyberangreb spreder sig.

Derfor har DI også taget initiativ til at samle de største cybersikkerhedsleverandører i Danmark for at drøfte mulighederne for, at deres viden i højere grad bliver bragt i spil til gavn for hinanden og for samfundets samlede sikkerhed. I den kommende tid vil DI arbejde videre for at understøtte større deling af trusselsinformation på tværs af det offentlige og private.

Platformen kan med fordel udvikles med afsæt i inspiration og læring fra andre lande, herunder Storbritannien.

DI anbefaler:

- Styrelsen for Samfundssikkerhed skal etablere en platform for fortrolig deling af trusselsinformation for virksomheder og myndigheder i Danmark. I første omgang skal fokus være på at sikre, at der deles mere trusselsinformation mellem aktører, der er i berøring med sikkerheden i den kritiske infrastruktur på tværs af sektorer eller står for sikkerheden i it-løsninger for mange organisationer, hvorefter scopet evt. kan udvides.

- Erhvervslivet, herunder særligt de større cybersikkerhedsleverandører, skal stille sig til rådighed for deling af relevant trusselsinformation på platformen, ligesom Styrelsen for Samfundssikkerhed skal dele relevant information om aktuelle cyberhændelser mod kritisk infrastruktur, som bliver lovpligtigt at indberette som følge af NIS2-direktivet.

- Brugerne af platformen skal verificeres, og det skal være muligt at dele indhold anonymt. Styrelsen for Samfundssikkerhed skal sikre, at informationen på platformen bearbejdes og filtreres, så den bliver tilstrækkelig operationel for brugerne, men skal samtidig tage hensyn til virksomheders forretningskritiske oplysninger.

- Derudover bør efterretningstjenesterne og øvrige myndigheder arbejde i retning mod at afklassificere flere oplysninger med henblik på at dele dem på

Eksempler på deling af trusselsinformation i andre lande

Storbritanniens National Cyber Security Centre (NCSC) driver portalen CiSP (Cyber Security Information Sharing Partnership). Denne portal er et samarbejde mellem staten og industrien, som har til formål at dele information om cybertrusler og sårbarheder. Formålet er at øge bevidstheden og reducere virkningen på britiske organisationer. CiSP giver medlemmer mulighed for at udveksle information i realtid på tværs af sektorer og organisationer.

På globalt plan findes trusselsdelingsplatforme såsom MISP Threat Sharing, som bl.a. er stiftet af EU. MISP er en open source-softwareplatform og består af et omfattende fællesskab af brugere, som deler oplysninger om trusler på tværs af lande. MISP omfatter flere initiativer, herunder software til at facilitere trusselsanalyse og informationsdeling samt frit tilgængelige strukturerede data om cybertrusler og taksonomier.

platformen eller alternativt etablere øvrige samarbejdsfora for øget deling af klassificeret information til gavn for samfundets samlede modstandsdygtighed over for cyberangreb.

- På platformen etableres også en fælles indgang til frivilligt at orientere offentligt om, at man er ramt af cyberangreb, så brugere og samarbejdspartnere kan finde pålidelig information samlet ét sted. I dag ligger denne information ofte tilgængelig på mange forskellige platforme og har tilmed været omgærdet af desinformation, hvor ondsindede aktører har haft interesse i at påstå angreb, der aldrig var sket.

- Med afsæt i trusselsinformationen på platformen kan myndighederne styrke sin kommunikation om det aktuelle trusselsbillede til den brede offentlighed, fx med inspiration fra Forsvarsakademiets deltagelse i "Krigens døgn".

Forslag 2: Indføring af et nationalt cyberfilter på internettrafik for at forhindre cyberangreb

Et såkaldt DNS-filter fungerer som et værn, der kan beskytte et helt netværk og give advarsler imod, at internetbrugeren tilgår skadelige domæner. Det kan være hjemmesider, der er kendt for alene at indeholde skadeligt indhold som virusprogrammer eller ransomware. Dermed mindskes risikoen for datatyveri, økonomiske tab og driftsforstyrrelser i en organisation. I modsætning til antivirusprogrammer, der kræver installation på hver enkelt enhed, kan et DNS-filter implementeres centralt og beskytte hele netværk i en organisation.

Den tekniske løsning bag DNS-filtrering er allerede moden og bruges i dag, men anvendelsen er stadig fragmenteret, og den frivillige del af DNS-beskyttelsen er ofte baseret på, at forbrugeren aktivt tilkøber det som ydelse – frem for at være bygget ind per default.

Ved at implementere et nationalt filter for myndigheder og udbrede brugen af DNS-filtrering på tjenesteudbyderniveau kan Danmark øge sin digitale modstandsdygtighed på en skalerbar og omkostningseffektiv måde. Samtidig understøtter løsningen bedre dataanalyse og udvikling af AI-drevne cybersikkerhedsinitiativer, der kan identificere og blokere trusler i realtid.

DI anbefaler:

- Digitaliseringsministeriet skal stille sig i spidsen for at sikre, at der udvikles og implementeres et centralt administreret DNS-filter for statslige myndigheder, der også kan stilles til rådighed for

kommuner og regioner. Dette skal understøtte en høj og ensartet sikkerhedsstandard i den offentlige sektor, hvor brugen af DNS-filtrering i dag er begrænset. Samtidig skal initiativet sikre, at "telefonbogen" – dvs. listen over domæner, der skal blokeres – løbende vedligeholdes og stilles til rådighed for branchen med henblik på at øge beskyttelsen i en bredere kontekst. Filteret bør administreres af staten i samarbejde med private leverandører med ekspertise i DNS-sikkerhed. Det estimeres, at en sådan løsning vil koste i omegnen af 25 mio. kr. pr. år samt implementeringsudgifter på ca. 5–10 mio. kr. Løsningen kan fx udvikles med inspiration fra det EU-støttede initiativ, DNS4GOV.

- Samtidig bør regeringen opfordre tele- og internetudbydere til at tilbyde DNS-beskyttelse som en indbygget del af deres tjenester. Et DNS-filter på tjenesteudbyderniveau vil muliggøre en ensartet og skalerbar sikkerhedsløsning på tværs af forskellige netværk og teknologier.

- DI vil tage initiativ til at samle branchen for at drøfte, hvilke tiltag der kan tages. DNS-filtrering kunne baseres på følgende:

    - Forbrugere og SMV'er bør tilbydes DNS-beskyttelse via en opt-out-model, hvor løsningen er aktiveret som standard, men kan fravælges.

    - Store virksomheder (enterprise-segmentet), der ofte har egne sikkerhedsløsninger, bør tilbydes en opt-in-model.

- Endelig bør tele- og internetudbydere opfordres til at dele anonymiserede data om cybertrusler med Styrelsen for Samfundssikkerhed. Dette vil styrke den nationale threat intelligence og muliggøre hurtigere og mere præcise reaktioner på cyberangreb.

Ny teknologi er et tveægget sværd i cyberspace

Teknologien udvikler sig hurtigere end nogensinde før, hvilket skaber nye ud-fordringer inden for cybersikkerhed, hvor AI har vist sig at udgøre en central og stigende trussel. Med kunstig intelligens' avancerede og let tilgængelige teknologi kan cyber-kriminelle hurtigt få adgang til værktøjer, der kan analysere store mængder data, ligesom kunstig intelligens kan bruges til at målrette og automatisere angreb.

Men AI har også et stort potentiale til at bidrage til vores resiliens. For eksempel kan AI anvendes til at simulere angreb til trænings-formål, analysere netværk, software og deslige for sårbarheder samt forhindre angreb ved at isolere eller blokere skadeligt indhold. Det er derfor essentielt, at AI ikke udelukkende betrag-tes som en trussel mod cybersikkerhed, men at vi også omfavner teknologien og opkvalificerer vores evner i brugen af AI til at kunne modstå fremtidige cybertrusler.

Forslag 3: Opproritering af forskning og innovation inden for cybersikkerhed

Hvis Danmark skal være på forkant med et stadigt mere avanceret trusselsbillede er der behov for at styrke forsknings- og innovationsmiljøerne inden for cybersikkerhed. Det kræver flere investeringer i forskning, flere undervisere og specialister og langt mere viden om, hvordan vi designer it-systemer, som i udgangspunktet er sikre og mindre sårbare over for menneskelige fejl end i dag.

Der er endvidere behov for en tættere sammenhæng mellem de danske uddannelsesinstitutioner og virksomheder, så vi både får løftet innovationshøjden på området og øget udbuddet og bredden af cyberkompetencer i Danmark.

DI anbefaler:

- Folketinget skal som en del af aftalen om forskningsreserven for 2026 foretage en markant opprioritering af forskning inden for fremtidens teknologi, herunder cybersikkerhed, med henblik på at udbygge forskningsmiljøerne og deres samarbejde med danske virksomheder inden for området.

- Som et første skridt skal der i 2026 afsættes en pulje på 500 mio. kr. under Innovationsfonden til forskning i kritiske og digitale teknologier, herunder cybersikkerhed. Derudover anbefaler DI, at regeringen inden for rammerne af de årlige forskningsreserver øremærker 1 mia. kr. til forskning og innovation i fremtidens teknologi på de danske forskningsinstitutioner i perioden 2026-2036 med særlig vægt på cybersikkerhed, kunstig intelligens, robot- og produktionsteknologi og kvantealgoritmer.

- Midlerne skal opdyrke og styrke danske styrkepositioner og sikre, at forskning og innovation inden for bl.a. cybersikkerhed tænkes sammen med udviklingen og udrulningen af øvrige kritiske teknologier. Nogle af de prioriterede indsatser kunne fx være kryptografi, automatiseret trusselsdetektion og zero-trust-arkitektur.

- Derudover skal Nationalt Koordinationscenter for Cybersikkerhed (NCC) bidrage til at sikre nemmere adgang til europæiske samarbejdsprojekter på cyberområdet for danske forskningsinstitutioner og virksomheder gennem styrket vejledning og udbredelse af viden om relevante puljer og ansøgningsprocesser. Samtidig bør de nationale cybersikkerhedspuljer kobles tydeligere op på strategisk vigtige fokusområder i den nationale cybersikkerhedsstrategi, så det sikres, at midlerne ikke smøres for tyndt ud, men bliver brugt der, hvor værdien er størst.

For DI er cyberområdet et prioriteret område inden for innovation og forskning, som vi løbende vil levere anbefalinger indenfor. Der henvises i øvrigt til forslaget fra Forskningsalliancen om opbygning af strategiske forsknings- og udviklingsprogrammer inden for forsvarsrelaterede nøgleteknologier, herunder cybersikkerhed, som skal finansieres inden for rammerne af forsvarsforliget. Forskningsalliancen er et samarbejde mellem Dansk Metal, Akademiet for de Tekniske Videnskaber (ATV), Ingeniørforeningen IDA og DI.

Forslag 4: Tværgående cyberberedskabsøvelser

MGod cybersikkerhed handler også om at have en klar plan for, hvad man gør, når man bliver ramt af et cyberangreb. Det gælder både på samfundsplan og i hver enkel organisation.

Engang blev de nationale krisestyringsøvelser afholdt hvert andet år, men det er ikke sket siden 2019. I regeringens beredskabsaftale fra januar fremgår det, at der afholdes en ny krisestyringsøvelse i 2025. Den bør naturligvis også have fokus på cyberangreb.

Til sammenligning afholdes der fire årlige operative cyberøvelser i Finland i samarbejde mellem JYVSECTEC (Jyväskylä Security Technology), som er et uafhængigt forsknings-, udviklings- og træningscenter og det finske Transport- og Kommunikationsministeriet og Sikkerhedsudvalg.

Hele Danmark Øver er en årligt tilbagevendende cyberberedskabsøvelse, der har til formål at give virksomheder et konkret indblik i, hvordan det er at stå midt i et cyberangeb for at klæde dem bedre på til at håndtere en reel krise. Bag initiativet står TDC Erhverv i et partnerskab med en aktører fra den offentlige og private sektor, herunder Styrelsen for Samfundssikkerhed, Industriens Fond, Dansk Erhverv, IT Branchen, Alm. Brand og Dansk Industri.

Der er et stort potentiale i at udbrede cyberberedskabsøvelser i en national kontekst for at øge den generelle awareness i samfundet og samtidig sikre en stærk koordination på tværs af sektorer med særligt fokus på kunne håndtere de mest kritiske angrebsscenarier på en effektiv måde.

3 ud af 4

af danskerne er enige eller meget enige i, at virksomhedernes ekspertise kan bidrage til at løse samfundsopgaver i krisesituationer.

Kilde: DI's befolkningspanel, marts 2025

Den kraftige stigning i hybridangreb betyder, at det i særlig grad er på tværs af det sektorielle ansvar, at der er brug for både øvelser og planer.

DI anbefaler:

- Ministeriet for Samfundssikkerhed og Beredskab skal koordinere, at der afholdes en årligt tilbagevendende cyberberedskabsøvelse, der både involverer myndigheder og relevante virksomheder med særligt fokus på at kunne håndtere alvorlige angrebsscenarier, der går på tværs af sektorer og involverer nedbrud i ét eller flere centrale it-systemer, der påvirker den kritiske infrastruktur.

- I tillæg til de nationale krisestyringsøvelser skal Cybersikkerhedspagten bidrage til udbredelsen af den frivillige cyberberedskabsøvelse, Hele Danmark Øver, for at sikre, at flere virksomheder bliver klar til at håndtere cyberangreb samtidig med, at tilslutningen øges blandt offentlige myndigheder, uddannelsesinstitutioner og andre civilsamfundsorganisationer, så vi får et bedre cyberberedskab på tværs af forskellige dele af samfundet.

Ny, omfattende norsk beredskabsplan

Den norske regering har i januar fremlagt en omfangsrig beredskabsplan med over 100 beredskabstiltag, der også berører cyberområdet. Konkret foreslår regeringen bl.a. at etablere en cyberberedskabsordning, hvor myndigheder, virksomheder og forskningsmiljøer samarbejder om at håndtere kriser.

Den private sektor bliver eksempelvis inddraget i arbejdet med en ny cyberberedskabsordning, hvor et offentligt-privat samarbejde vil blive igangsat. I forlængelse heraf iværksættes en strategi for at styrke modstandskraften mod desinformation.

Forslag 5: Cyberberedskabsordning til at dele IT-eksperter i tilfælde af større cyberangreb

Manglen på IT- og cyberspecialister udgør allerede i dag et problem. Det vil være akut problematisk, hvis Danmark rammes af et større, nationalt cyberangreb, og de offentligt myndigheder vil sandsynligvis ikke kunne håndtere et sådant angreb alene. En cyberberedskabsordning skal imødegå manglen på cyberspecialister ved at myndigheder og virksomheder samarbejde om kriser, når de opstår, så man kan udnytte de samlede cyberkompetencer, der er til rådighed i samfundet.

DI anbefaler:

- Ministeriet for Samfundssikkerhed og Beredskab bør senest i 2026 etablere en cyberberedskabsordning med eksperter fra både virksomheder, offentlige myndigheder og universiteter, der skal samles i tilfælde af større, nationale cyberhændelser.

- Cyberordningen skal fungere på den måde, at medarbejdere fra virksomheder og videregående uddannelsesinstitutioner skal kunne aktiveres via stand-by kontrakter, der skal indgås med offentlige myndigheder på forhånd. En virksomhed eller en uddannelsesinstitution kan således "leje" medarbejdere ud i en periode, hvis – eller når – et nationalt cyberangreb opstår.

- Stand-by kontrakterne skal sendes i udbud for at sikre åben og lige konkurrence. Det er op til den enkelte virksomhed eller institution om man vil byde ind på en sådan kontrakt.

Teknologi, sikkerhed og konkurrenceevne i en ny geopolitisk virkelighed

En ændret geopolitisk situation og hastige udviklinger i den digitale verden betyder, at sikkerhed og autonomi står øverst på dagsordenen i de kommende år. Teknologi er blevet centrum for stormagternes konkurrence, og det stiller øgede krav til vores sikkerhed og robusthed, idet vores digitale afhængigheder og sårbarheder bliver stadigt tydeligere.

Den nye situation understreger, at vi i Europa skal kunne mere på egen hånd. Det gælder også på den teknologiske front. Det er derfor vigtigt, at vi tager de nødvendige skridt for at styrke innovationen inden for kritiske teknologier, så vi kan lukke det teknologiske gab.

I takt med at digitale løsninger bliver mere integrerede i både økonomi og sikkerhed, opstår nye udfordringer, som kræver strategisk håndtering for at sikre vores konkurrenceevne og sikkerhed. Her skal vi naturligvis overveje, hvordan vi bedst muligt styrker Danmarks såvel som EU's digitale robusthed og konkurrenceevne og undgår kritiske afhængigheder, så vi ikke låses fast til én juridisk eller teknologisk ramme. I samme ombæring må vi ikke afskære os fra de nyeste teknologier og de mest konkurrencedygtige løsninger.

Vi kommer ikke nødvendigvis til at kunne alt selv, men grundlæggende skal vi arbejde for et mere uafhængigt Europa. Til at understøtte Europas teknologiske autonomi må vi investere og understøtte indsatser målrettet kritiske teknologier som AI, cloud, halvledere, kvanteteknologi, cyberteknologi, supercomputere samt 5G og kommunikationsnetværk. Vi skal i EU være langt bedre til at udvide og udnytte det digitale indre marked til at skabe de nødvendige fremskridt. Det skal ske samtidig med, at vi sikrer adgang til den nyeste teknologi uden at gå på kompromis med cybersikkerhed.

Dette er ikke alene en vigtig forudsætning for at styrke vores konkurrencekraft, men også en forudsætning for, at virksomhederne kan vælge netop de løsninger, der passer til dem.

Illustrative tal:

Internationalt ser vi forskellige strategier for teknologisk suverænitet. USA og Kina investerer målrettet i teknologisk autonomi , mens Europa i høj grad er afhængige af udenlandske løsninger.

92 % af vestens data opbevares i USA, hvor amerikanske virksomheder har ca. 69 % af markedet for cloud-infrastruktur i Europa.

Dækningen med 5G Standalone (SA)-netværk var i Europa kun 40 % ved udgangen af 2024, mens Nordamerika nåede 91 %, og Asien og Stillehavsområdet 45 %.

AI-investeringer, tegner EU sig kun for 7 % af det globale marked, mens USA og Kina tilsammen står for 72 %.

Europa producerer kun 10 % af verdens halvledere, hvilket er betydeligt mindre end de 54 %, der fremstilles i Taiwan og de 16 %, der produceres i Kina.

Kilde: Connect Europe (2025), Europa-Parlamentet/Sarah Knafo rapport om teknologisk suverænitet (2025).

Digitale balancer og veje frem

Virkeligheden er, at den offentlige og private sektor er tæt forbundne og gensidigt afhængige af hinanden. På samme måde er vi også afhængige af internationale virksomheder, der historisk og fortsat understøtter vores konkurrenceevne og sikkerhed – særligt det transatlantiske samarbejde.

DI mener ikke, at organisationer bør undgå bestemte leverandører eller afkoble sig fra amerikanske teknologier. Det mener vi heller ikke er realistisk på kort sigt. De geopolitiske forandringer skaber dog en situation, der kræver noget nyt af os. Det må vi forholde os strategisk og kløgtigt til. Det er blot sund fornuft.

Uagtet det politiske billede bør man som virksomhed:

- **Løbende vurdere den politiske udvikling**
- **Kortlægge digitale sårbarheder og værdikæder samt foretage risikovurderinger med fokus på data- og cybersikkerhed**
- **Overveje exit-strategier for kritiske teknologier**
- **Udarbejde beredskabsplaner for teknologisk robusthed og cybersikkerhed**

2. Cybersikkerhedsløsninger til SMV'er

Danske virksomheder er generelt ikke nok rustet til at håndtere de aktuelle risici, der følger med det nuværende trusselsbillede på cyberområdet, men særligt én målgruppe er mest sårbar.

Mere end 9 ud af 10 danske virksomheder er små og mellemstore virksomheder (SMV'er) med mindre end 250 ansatte. For dem er hele forretningen typisk på spil, når de rammes af cyberangreb, men ofte har de ikke selv ressourcerne til at opbygge den fornødne modstandsdygtighed i forretningen.

Der er allerede flere tiltag i gang for at styrke cybersikkerheden hos SMV'erne, men vi ser samtidig, at udviklingen går langsomt, selvom trusselsbilledet er stigende og i konstant forandring. Det kalder på en ny tilgang til cybersikkerheden for denne type af virksomheder, hvor der samtidig tages højde for, at SMV'er i praksis er en bred kategori af virksomheder, der har meget forskelligartede behov. Her har erhvervslivet sammen med myndighederne en afgørende rolle at spille ved at sikre konkrete og målrettede værktøjer, der kan bidrage til at løfte sikkerheden i de mindste virksomheder i Danmark.

Forslag 6: Enhed for SMV'ers cybersikkerhed – styrket overblik, målrettet vejledning og genvej til handling

For at løfte samfundets samlede robusthed over for cyberangreb er der behov for, at vi i fællesskab sænker barriererne for SMV'ernes arbejde med cybersikkerhed og i højere grad tilrettelægger indsatserne, så de matcher forskellige typer virksomheders behov og modenhed.

Der findes allerede en del værktøjer til at løfte cybersikkerheden, men det er nødvendigt at samle denne viden og gøre værktøjerne mere anvenderorienterede og målgruppespecifikke i tråd med forskelligartede SMV-behov. Derudover er der behov for en stærk mobiliseringsindsats for at sikre, at værktøjerne faktisk når ud til forskellige typer af SMV'erne og bruges til at løfte cybersikkerheden i praksis.

Det kalder på en samling af økosystemet af private og offentlige cybersikkerhedsløsninger til SMV'er, så vi sammen sikrer klare veje til et løft af den basale cybersikkerhed hos den enkelte virksomhed.

40 pct. af SMV'erne har ikke et højt nok digitalt sikkerhedsniveau ift. deres risikoprofil.

Kilde: Styrelsen for Samfundssikkerhed, Digital sikkerhed for SMV'er (2024), december 2024

DI anbefaler:

- DI opfordrer til, at der skal etableres et offentligt-privat samarbejde om oprettelsen af en enhed, der skal fungere som samlet indgang for små og mellemstore virksomheders arbejde med cybersikkerhed. Formålet er at give flest mulige danske SMV'er en grundforståelse og -kompetencer inden for cybersikkerhed til gavn for både erhvervslivet og samfundets samlede robusthed – og ad den vej også stimulere efterspørgslen efter markedsdrevne cybersikkerhedsløsninger og rådgivning til SMV'er.

- For det første skal enheden arbejde for, at viden om det aktuelle trusselsbillede og relevante værktøjer løbende opdateres med udgangspunkt i SMV'ernes behov og modenhed. I den forbindelse skal en national koalition af private og offentlige aktører gå sammen om at forbedre de eksisterende cybersikkerhedsværktøjer og -træning for at sikre væsentligt mere konkret, anvenderorienteret vejledning målrettet behovene i forskellige typer af SMV'er. De basale værktøjer stilles gratis til rådighed og samles på én platform.

- For det andet skal enheden arbejde vedvarende og proaktivt for, at de rette informationer og værktøjer faktisk når ud til de relevante målgrupper og bliver omsat til et løft af cybersikkerheden på en måde, der understøtter den enkelte virksomheds behov og modenhed. Enheden skal i den forbindelse skabe overblik over relevante tilbud, der kan hjælpe SMV'erne videre ved at pege på konkrete næste skridt til at styrke cybersikkerheden efter at have benyttet de grundlæggende værktøjer. Det kunne eksempelvis være D-mærket og andre relevante løsninger på cybersikkerhedsmarkedet. Endvidere vil enheden kunne bidrage til modningen af leverandørmarkedet ved at pege på behov i målgruppen, som ikke dækkes af eksisterende løsninger.

- DI deltager aktuelt i en projektgruppe med Industriens Fond, Security Tech Space, Alexandra Instituttet og Styrelsen for Samfundssikkerhed, som afdækker det nærmere scope, governance og finansieringsstruktur for SMV-enheden med inddragelse af en bred vifte af eksperter. DI opfordrer i den forbindelse Ministeriet for Samfundssikkerhed til at sikre offentlig medfinansiering af SMV-enheden som led i den nationale cyberstrategi.

- Med afsæt i et styrket samarbejde med øvrige aktører forpligter DI sig til at bidrage med at sikre, at SMV-tilbud og -vejledning er praksisnære og modtagerorienterede samt at mobilisere SMV'er på basis af erfaringer fra andre centrale dagsordener.

Forslag 7: Styrket offentligt-privat samarbejde om udviklingen af D-mærket

Danmarks mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse, D-mærket, er et vigtigt redskab til at løfte sikkerhedsniveauet i danske virksomheder og forsikre forbrugere, kunder og samarbejdspartnere om, at de er i sikre hænder.

D-mærket henvender sig til virksomheder uanset størrelse, men er særligt for SMV'er et godt værktøj til bl.a. at skabe overblik over krav til at imødegå cybersikkerhedsrisici og sætte ind dér, hvor effekten af tiltag er størst. Samtidig er D-mærket en oplagt mulighed for at understøtte implementeringen og mindske dokumentationsbyrden i forbindelse med NIS2. En barriere for udbredelsen af D-mærket er, at mange danske virksomheder opererer på flere markeder og derfor har brug for en europæisk mærkningsordning.

D-mærket er født som et offentligt-privat samarbejde, men der er stadig et stort uforløst potentiale i styrke samarbejdet for at sikre, at mærkningsordningen bliver et fælles referencepunkt på tværs af hele Danmark og resten af EU.

DI anbefaler:

- DI opfordrer til, at Ministeriet for Samfundssikkerhed og Beredskab stempler tydeligere ind i det offentlige-private samarbejde om udviklingen og udbredelsen af D-mærket. Som et første skridt skal mærket anerkendes fra officielt hold i tråd med fx Svanemærket.
- På nationalt plan betyder det særligt, at den danske implementering af NIS2 og tilhørende tilsyn samtænkes med D-mærket, så D-mærket fra officielt hold anerkendes som et konkret værktøj, der hjælper virksomheder og organisationer med at leve op til NIS2. Særligt for SMV'er vil det kunne lette implementeringen og dokumentationsbyrden væsentligt, at tilsynsmyndighederne accepterer D-mærket som dokumentation for efterlevelse af NIS2-kravene.
- På europæisk plan kan Ministeriet for Samfundssikkerhed og Beredskab bistå indsatsen for at skabe fundamentet for en fremtidig europæisk mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse. Konkret skal ministeriet under det danske EU-formandskab tage initiativ til at drøfte og igangsætte et arbejde for udformningen af en fælles europæisk mærkningsordning, der kan bidrage til byrdelettelser for erhvervslivet ved at standardisere kravene til databeskyttelse, it-sikkerhed og dataetik på tværs af EU og gøre det langt nemmere for virksomhederne at dokumentere regelefterlevelse på tværs af regulativer. Til sammenligning er man fra officielt hold i Belgien meget aktive i den europæiske interessevaretagelse for at løfte en belgisk løsning op som et accepteret fælleseuropæisk stempel, som viser NIS2-compliance.

D-mærket – en genvej til at styrke cybersikkerheden i virksomheder

D-mærket er skabt for at hjælpe virksomheder med at tydeliggøre deres digitale ansvarlighed, så forbrugerne kan opleve digital tryghed. D-mærket er den første mærkningsordning, der med afsæt i internationale standarder kombinerer både it-sikkerhed og ansvarlig dataanvendelse i ét mærke, der er relevant for alle typer og størrelser af virksomheder.

Mærkningen er med til at gøre det nemmere for virksomheder at navigere i det digitale landskab og sikre, at de lever op til de nødvendige standarder for at beskytte data og privatliv samt hjælpe med at blive rustet til at stå bedre imod hackerangreb.

D-mærket er skabt af Industriens Fond i samarbejde med Dansk Industri, Dansk Erhverv, SMVdanmark og Forbrugerrådet Tænk. D-mærket er en uafhængig privat organisation.

Anbefalingen om etablering af D-mærket stammer fra den regeringsnedsatte Ekspertgruppe om dataetik. I forbindelse med lanceringen af D-mærket udtalte Erhvervsminister Simon Kollerup: *"Det er mit håb, at det nye mærke bliver for de digitale virksomheder, hvad økomærket er for fødevarebranchen: en blåstempling, som virksomhederne markedsfører sig på, og som forbrugerne navigerer efter."*

Et tegn på troværdighed og symbol på kvalitet

digital tryghed

3. Uddannelse og cyberkompetencer

Danske virksomheder og myndigheder navigerer i en kompleks tid præget af hurtig teknologisk udvikling, langt mere avancerede og automatiserede cyberangreb og meget ny regulering på cyberområdet. Og allerede i dag er der mangel på cyberkompetencer til at løse opgaverne.

Den problematik vil kun blive større i fremtiden, hvor der bliver øget efterspørgsel på specialiserede kompetencer til at løfte sikkerhedsniveauet – både i de tekniske løsninger, men også til at efterleve lovgivning, foretage risikovurderinger og sikre den organisatoriske forankring af cybersikkerhedstiltag.

Forslag 8: Uddan flere IT- og cybersikkerhedseksperter

Flere af de nødvendige tekniske løsninger til at styrke cybersikkerheden i virksomheder og organisationer findes allerede i dag – men uden kvalificerede medarbejdere, som kan implementere og vedligeholde dem, forbliver de uudnyttede. Der er derfor behov for en styrket og målrettet indsats for at uddanne flere cybersikkerhedseksperter i Danmark.

Det kræver at universiteterne ikke er nødsaget til at afvise kvalificerede ansøgere på it-uddannelser på grund af dimensioneringer, der ikke tager hensyn til arbejdsmarkedets behov.

Ved studieoptaget i sommeren 2024 blev mere end 250 kvalificerede førsteprioritetsansøgere afvist fra en ikke-ledighedsdimensioneret IT-uddannelse på et universitet, som de ellers var både interesserede i og kvalificerede til at påbegynde.

DI anbefaler:

- Regeringen og forligskredsen skal prioritere flere studieplader på de relevante bachelor- og kandidatuddannelser, så der uddannes flere IT-eksperter i hele landet.

- Det skal sikres, at alle kvalificerede førsteprioritetsansøgere optages på ikke-ledighedsdimensionerede STEM-uddannelser. Det vil kræve, at der afsættes 50.000 kr. pr. plads, svarende til 75 mio. kr. årligt.

- Sektordimensioneringen af studiepladser på universiteterne skal tilgodese arbejdsmarkedets behov for it-specialister både nu og i fremtiden.

Derudover er efter- og videreuddannelse inden for cybersikkerhed afgørende. Der er allerede et stort udbud af efter- og videreuddannelsestilbud på dette område, og der kommer løbende flere til, bl.a. inden for mikro-certificeringer i IT-sikkerhed og nye fagmoduler i digital sikkerhed for generalister. Det er i den forbindelse vigtigt, at alle aktører bidrager til at sikre større udbredelse af de eksisterende tilbud, ligesom tilbuddene løbende skal opdateres i takt med ændringerne i trusselsbilledet.

Forslag 9: Styrket fokus på cybersikkerhed på tværs af universitetsuddannelserne

Universiteterne spiller en central rolle i at forbedre den nationale cybersikkerhed, da de uddanner fremtidige medarbejdere – både til virksomheder, som efterspørger højt specialiserede cyberkompetencer, men også til det bredere erhvervsliv, hvor der er behov for at højne sikkerhedskulturen.

DI anbefaler:

- Universiteterne indfører et obligatorisk basiskursus i digital sikkerhed som en del af introforløbet for nye studerende på alle universitetsuddannelser. Kurset skal højne den generelle awareness for de højtuddannede og styrke fokusset på en sikker omgang med universiteternes egne it-systemer, som indeholder mange kritiske data, herunder forskningsdata.

- For det andet foreslås det at indføre obligatoriske ECTS-udløsende fagforløb i cybersikkerhed på alle it-relaterede universitetsuddannelser i Danmark, hvor det ikke findes i forvejen, for at sikre, at sikkerhedsrisici tænkes ind i alt fra it-projektledelse til softwareudvikling. Det ECTS-udløsende fag foreslås finansieret inden for rammerne af forsvarsforliget.

DI vil også fortsat have fokus på, at forløb om cybersikkerhed indgår på de korte og mellemlange it-uddannelser i det omfang, at dette ikke allerede er tænkt ind. DI støtter i den forbindelse også, at Uddannelses- og forskningsministeren netop godkendt tre nye professionsbacheloruddannelser i cybersikkerhed.

4. Stærk national sikkerhedskultur

Mange brud på IT-sikkerheden skyldes menneskelige fejl og uopmærksomhed, og der er derfor behov for at styrke sikkerhedskulturen i Danmark gennem øget awareness og et generelt løft af kompetencer til at modstå cyberangreb og digital svindel i den brede befolkning.

En robust sikkerhedskultur kræver, at alle dele af samfundet er bevidste om cybertruslens alvor og ved, hvordan de bedst kan beskytte sig selv og deres organisationer mod angreb.

En højnet generel bevidsthed om vigtigheden af digital sikkerhed i befolkningen kan skabe en stærk og modstandsdygtig digital frontlinje, der ikke blot beskytter os mod de aktuelle cybertrusler, men også gør os parate til at imødegå fremtidige angreb.

Forslag 10: Målret den offentlige oplysningsindsats, så den når ud til alle borgere og virksomheder

Der findes allerede meget information på offentlige hjemmesider, der kan hjælpe borgere og virksomheder i retning af en mere sikker digital adfærd, ligesom myndighederne løbende laver oplysningskampagner for at øge den generelle awareness i befolkningen, bl.a. om nye tendenser i cyberangreb og svindelforsøg.

Over de kommende år er det afgørende, at den tilgængelige information i højere grad målrettes forskellige befolknings- og virksomhedsgrupper og faktisk når ud til målgrupperne. Det kræver, at informationen i højere grad kanaliseres ud via de organisationer, som borgere og virksomheder er engageret i.

DI anbefaler:

- Indsatsen for vejledning og oplysning i regi af sikkerdigital.dk styrkes med 10 mio. kr. årligt. Midlerne skal bruges til en målrettet oplysnings- og awarenessindsats, hvor Styrelsen for Samfundssikkerhed og Beredskab i langt højere grad samarbejder med relevante civilsamfunds- og brancheorganisationer for at nå ud til alle virksomheds- og borgergrupper i samfundet, herunder de mindste virksomheder i Danmark. Et oplagt sted at forankre og koordinere en styrket oplysningsindsats er i Cybersikkerhedspagten.

- Indsatsen skal sikre, at informationen ikke blot er til stede på sikkerdigital.dk, men også bliver bragt i spil for at udbrede basale cybersikkerhedstiltag i praksis. I den forbindelse stiller DI sig til rådighed for at udbrede sikkerhedskampagner målrettet medlemmer af Dansk Industri.

- Den SMV-rettede del af oplysningsindsatsen skal koordineres med enheden, der skal understøtte cybersikkerheden hos SMV'erne (forslag 6).

Forslag 11: Public service-institutionerne skal lave mere indhold om digital sikkerhed

Public service-institutionerne (DR, TV2 og de regionale TV2-virksomheder) har bl.a. til opgave at sikre den danske befolkning nyhedsformidling, oplysning og undervisning, og kan spille en central rolle i at oplyse og uddanne befolkningen i bedre at forstå cybertruslen, og hvordan man som borger og virksomhed kan bidrage til at øge sit digitale forsvar. Særligt DR har en central rolle i at informere borgerne, hvis Danmark rammes af hybride angreb.

DI anbefaler:

- Public service-institutionerne skal udvikle indhold, der har til formål at oplyse borgerne om det aktuelle trusselsbillede, herunder fra cybertrusler og aktuelle mis- og desinformationskampagner fra fremmede aktører. Institutionerne skal desuden uddanne befolkningen i at navigere i nyheder og information på internettet, herunder kritisk stillingtagen til kilder, afsendere og mulige intentioner i indhold, uddanne befolkningen i at genkende indhold, der er genereret af AI og særligt med det formål at udbrede fake news eller andet vildledende indhold samt informere virksomheder om konkrete og aktuelle kampagner, der kan have betydning for deres forretningsmæssige sikkerhed. Se også DI's første beredskabspolitiske udspil Kriser kommer aldrig belejligt.

- Udviklingen af nyt indhold skal prioriteres inden for rammerne af en ny medieaftale, som skal gælde fra 2026. Kravet bør løftes ind i den nye Public Service-kontrakt og gælde fra 2026 og frem, hvor den nuværende kontrakt udløber.

Foto: Adobe Stock

Internationale indsatser for styrket cybersikkerhed

Cybertruslen er grænseoverskridende i sin natur, og vi har allerede set mange eksempler på cyberangreb, der har haft vidtrækkende konsekvenser på tværs af utallige lande. Samtidig ændrer nye teknologier såsom AI og kvanteteknologi fundamentalt ved måden at føre moderne krig på. Det stiller store krav til cybersikkerheden i forsvarssystemerne.

Når truslerne er globale, må mange af vores svar også være det.

EU tager vigtige skridt for at styrke medlemslandenes sikkerhed

I en ny hvidbog om fremtiden for det europæiske forsvar peger EU-kommissionen på digitale kompetencer, herunder AI-, kvante- og cyberområdet som ét ud af syv prioriterede områder, hvor det europæiske forsvar skal styrkes markant. Samtidig fremhæver EU's nye beredskabsstrategi nødvendigheden af at styrke samarbejdet mellem offentlige myndigheder og private aktører og vigtigheden af at integrere civile og militære kapaciteter langt mere.

Ét af de afgørende skridt i den forbindelse er at styrke den europæiske innovation og industri inden for cybersikkerhedsløsninger med dual use-potentiale. Her har EU allerede en række investeringsprogrammer, men støtten er i dag fragmenteret, og det er svært for nye aktører at komme ind i økosystemet.

Den danske regeringen kan i EU-regi arbejde for, at EU accelererer investeringerne i dual-use cybersikkerhedsteknologier, som kan modnes og overføres til operationel brug i både EU- og NATO-regi. Det kan ske gennem en EU-investeringsramme til udvikling af europæiske dual use-teknologier, som samler midler fra eksisterende fonde og programmer, herunder Digital Europe, European Defence Fund og Horizon.

Eksempler på prioriterede teknologiområder kunne være:

- Avanceret kryptering og security-by-design
- AI-baseret trusselsdetektion og beslutningsstøtte
- Kvantesikre løsninger
- Sikker kommunikation og datadeling mellem forsvar og civil sektor

Der er også et stort potentiale for at øge beredskabssamarbejdet med særligt de nordiske lande for at sikre et effektivt samspil om håndteringen af grænseoverskridende cyber- og hybridangreb.

NATO's digitale transformation frem mod 2030

Cyberforsvar er en del af NATO's kerneopgave med afskrækkelse og forsvar. NATO's fokus på cyberforsvar er rettet mod at beskytte sine egne netværk, operere i cyberspace (herunder gennem Alliancens operationer og missioner), hjælpe allierede med at forbedre deres nationale modstandsdygtighed og give mulighed for politisk samarbejde og kollektiv handling.

I 2016 anerkendte de allierede cyberspace som et operationelt domæne for NATO, i 2023 lancerede man NATO's Virtuelle Cyber Incident Support Capability (VCISC) for at støtte nationale indsatser til at forebygge cyberangreb, og i 2024 blev NATO's Integrated Cyber Defence Centre oprettet.

Frem mod 2030 fokuserer NATO på kritiske teknologiområder som cybersikkerhed og cyberspaceteknologier, dataudnyttelse og cloudcomputing.

Danmark kan spille en central rolle i denne udvikling, særligt gennem NATO Digital Foundry – en ny platform, der skal accelerere teknologiadoption og styrke samarbejdet mellem NATO, industrien, forskningsmiljøer og medlemslandene.

NATO's fokus er militært og operativt, men for at lykkes med at integrere ny teknologi effektivt, er det afgørende med et velfungerende civilt økosystem, hvor nye løsninger kan modnes og testes. Det er netop her, at EU's rolle som innovationsmotor og koordinator i det civile domæne supplerer NATO's militære orientering.

Ved at deltage aktivt i NATO's teknologiske udvikling kan Danmark udnytte sine styrkepositioner inden for cyber og digitalisering, samtidig med at vi styrker vores fælles forsvar mod cybertrusler.

Danmark deltager også i The European Centre of Hybrid Excellence, der er en selvstændig organisation, som bl.a. arbejder for at styrke samarbejdet mellem EU og NATO omkring hybride trusler. Forsvarsministeriet har endnu ikke udsendt permanente medarbejdere til centeret, på trods af de senere års stigende omfang af hybride trusler. Det kan man med fordel ændre på for at styrke den danske kapacitet på området.

Dansk Industri