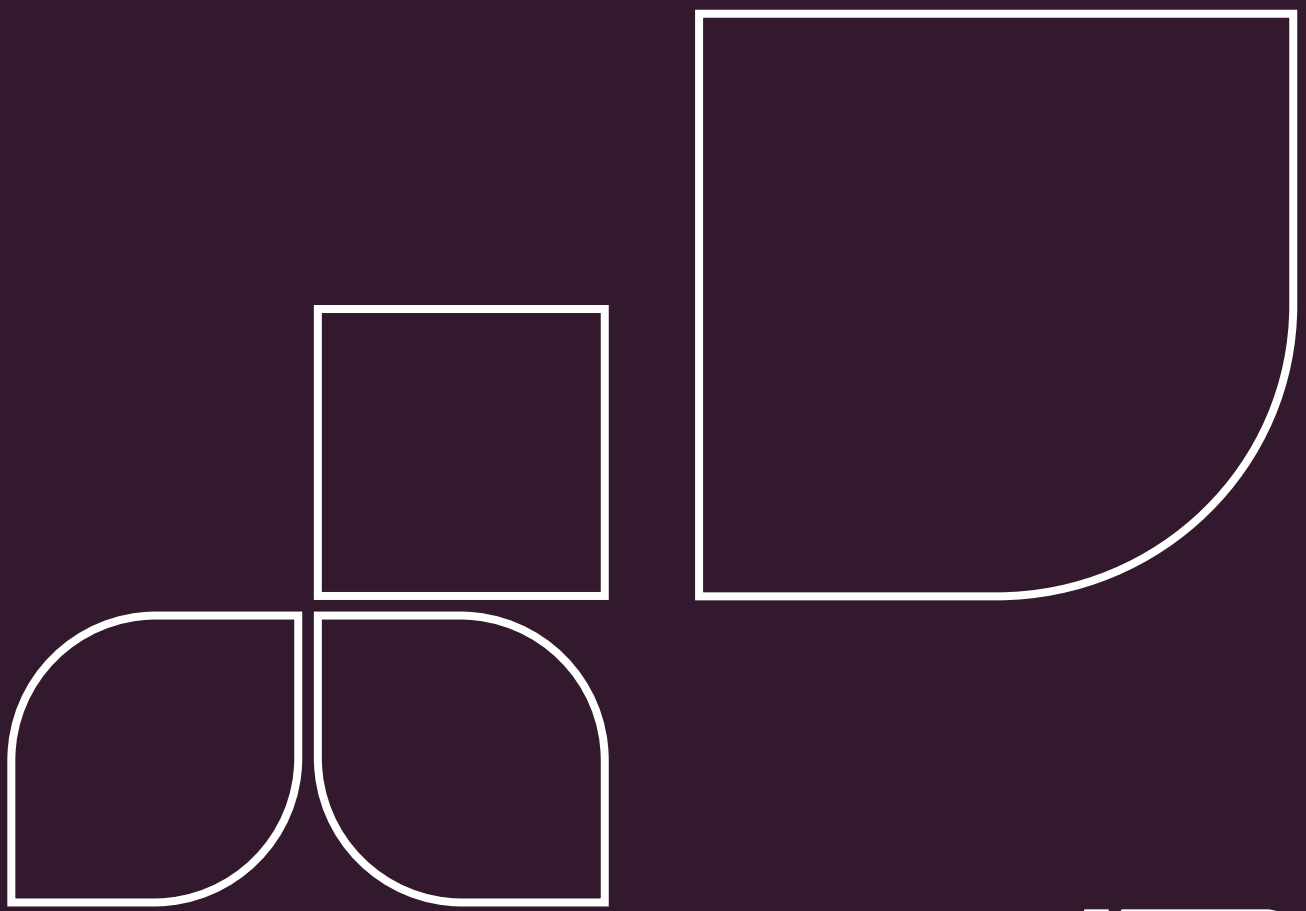
FREMTIDENS BESKYTTELSE AF DET DIGITALE DANMARK



IT-BRANCHEN

ITB.DK

Fremtidens beskyttelse af det digitale Danmark

Det geopolitiske trusselbillede, som Danmark står overfor nu og i fremtiden, er væsentligt ændret og byder på en mere fragmenteret verdensorden præget af stormagtsrivalisering med en militær og civil konkurrence på områder som økonomi, energi, teknologi og innovation. Mange af fremtidens konflikter vil formentlig ikke tage form af trusler mod Vesten om direkte åben militær konfrontation, men vil foregå i en gråzone med anvendelse af hybride trusler, som dækker over meget varierede ikke-militære sikkerhedspolitiske virkemidler som fx irregulære militære styrker ("små, grønne mænd"), desinformation via sociale medier, manipulation af den demokratiske samtale, påvirkning af valghandlinger, sabotage, økonomiske foranstaltninger og ikke mindst cyberangreb. Samtidig må det forventes, at fjendtligt indstillede stater i stigende omfang anvender spionage rettet mod både myndigheder og virksomheder, bl.a. for at imødegå konsekvenserne af sanktioner på teknologioverførsler.

I takt med den teknologiske udvikling og den stigende digitalisering udgør cyberangreb en stadig større trussel. Hertil er Danmark et af de mest digitaliserede lande i verden, og derfor er vi ekstra sårbare over for cyberangreb. Samtidig har vi i årevis underinvesteret i cybersikkerhed. Derfor er det også afgørende, at en styrkelse af Danmarks digitale forsvarsevne bliver et centralt omdrejningspunkt i de politiske forhandlinger om et nyt forsvarsforlig og en væsentlig del af Danmarks forsvarsindsats i fremtiden.

Forsvaret er underbemidlet og har en stor teknologisk gæld, men samtidig er vi nødt til at anlægge en bredere tilgang til sikkerhed. Samfundssikkerheden afhænger af, at civilsamfundets ressourcer tænkes mere systematisk ind både før, under og efter krise- og sikkerhedshændelser, så vi styrker vores sikkerhed både lokalt og nationalt. Det gælder ikke mindst, når vi taler om cybersikkerhed, som vores samfundssikkerhed i høj grad er bundet op på, da næsten al kritisk infrastruktur afhænger af digitale løsninger.

Med dette udspil foreslår IT-Branchens Policy Board for Cybersikkerhed fire strategiske indsatsområder og tilhørende 19 konkrete initiativer, som skal styrke Danmarks cyberforsvar og -robusthed.

De fire strategiske indsatsområder er følgende:

1. Styrkelse af robustheden i offentlige it-systemer og kritisk, national infrastruktur
2. Styrkelse af cyberforsvaret i danske virksomheder
3. Øget og accelereret uddannelse af danskere med cybersikkerhedskompetencer
4. Øget digitalisering og cybersikring af det danske forsvar.

FAKTAARK
IT-BRANCHENS 4 FORSLAG

Fremtidens beskyttelse af det digitale Danmark 2023
En international verdensorden i forandring og den hastige teknologiske udvikling har medført, at Danmark står overfor et skærpet, hybridt trusselsbillede, hvor truslerne ændrer karakter og stiller nye krav til forsvar og sikkerhed.

IT-Branchens Policy Board for Cybersikkerhed har identificeret fire strategiske indsatsområder og foreslår 19 konkrete initiativer, der skal styrke Danmarks cyberforsvar og -robusthed.

1

Styrkelse af robustheden i offentlige it-systemer og kritisk, national infrastruktur
Kritisk infrastruktur er digital infrastruktur, og vi skal være bedre beredt på cyberangreb, der har til formål at kompromittere eller skade samfundsvigtige funktioner i Danmark. Der er bl.a. behov for, at vi øger investeringsniveauet og optimerer organiseringen samt forpligtelsen til at efterleve en rækkes ensartede sikkerhedskrav på tværs af offentlige myndigheder, så vi kan afhjælpe teknologisk gæld og højne cybersikkerhedsniveauet i kritiske, offentlige it-systemer og infrastruktur.

2

Styrkelse af cyberforsvaret i danske virksomheder
Danske virksomheder er i stigende grad mål for cyberangreb og -kriminalitet. Der er bl.a. behov for et styrket offentlig-privat samarbejde om deling af viden om cybertrusler og -hændelser samt hjælp til virksomhederne til håndtering af disse. Der skal etableres en målrettet indsats for at sikre et minimumsniveau af cybersikkerhed i SMV'erne samt hurtig og effektiv implementering af NIS2-direktivet for berørte virksomheder.

3

Øget og accelereret uddannelse af danskere med cybersikkerhedskompetencer
Manglen på kompetencer en kæmpe hæmsko for cybersikkerheden i Danmark. Der er bl.a behov for akut investering i uddannelse af flere cyberspecialister samt generel opkvalificering og efteruddannelse af flere medarbejdere inden for cybersikkerhed. Der er også behov for tiltag målrettet øget rekruttering og fastholdelse af it- og cybersikkerhedskompetencer i Forsvaret.

4

Øget digitalisering og cybersikring af det danske forsvar
Der er behov for et betydeligt løft af Forsvarets digitale rygrad og interoperabilitet. Det indebærer bl.a. en nedbringelse af teknologisk gæld, øget cybersikring, øget offentlig-privat samarbejde om udvikling, anvendelse og certificering af dansk teknologi og IP samt øget budget til forskning og udvikling inden for fx kvanteteknologi, krypteret kommunikation og avanceret cybersikkerhed mhp. at opbygge selvstændige kapabiliteter og styrke dansk forsvarsindustri.

1 Styrkelse af robustheden i offentlige it-systemer og kritisk, national infrastruktur

Vi skal være bedre beredt på alle former for cyberangreb, der har til formål at kompromittere eller skade samfundsvigtige funktioner i Danmark. Sikkerhedsniveauet i dag er for lavt. Ifølge Statens it-projektråd har en stor andel af de samfundskritiske, offentlige it-systemer ikke tilfredsstillende it-sikkerhed, og flere statslige myndigheder lever ikke på til de tekniske minimumskrav til it-sikkerhed. Senest har også Rigsrevision udtalt kraftig kritik i en beretning om it-beredsskabet for i alt 13 samfundskritiske systemer. Også i regionerne og kommunerne halter det med it-sikkerheden. Ordentlig cybersikkerhed i de offentlige it-systemer er vital for at bevare borgernes tillid til systemerne og dermed sikre opbakning til fortsat digitalisering og effektive digitale løsninger.

IT-Branchens cybersikkerhedsboard foreslår følgende handlinger:

- Et markant **øget investeringsniveau**, der skal afhjælpe teknisk gæld og højne cybersikkerhedsniveauet i kritiske, offentlige it-systemer og infrastruktur, så vi er bedre sikret mod økonomiske og samfundsmæssige konsekvenser af destruktive cyberangreb. Herunder fokus på rettidig og fuld implementering og efterlevelse af NIS2 for berørte myndigheder og kritisk infrastruktur.

- **Obligatoriske cybersikkerhedskurser i den offentlige sektor** med information om, hvordan medarbejdere modstår phishing, gør korrekt brug af passwords mv. og hvordan ledelsen skal sikre organiseringen af cybersikkerhedsarbejdet.

- **Øget forpligtelse og koordination mellem myndigheder på tværs af stat, regioner og kommuner.** Dette fx hjulpet på vej af en centralisering af myndighedsansvar og ansvar for udmøntning af midler og initiativer inden for cybersikkerhed, hvilket bl.a. skal sikre, at de offentlige myndigheder lever op til nogle ensartede cybersikkerhedskrav. Hertil bør kommunerne omfattes af NIS2-direktivet.

- **Øget fokus på offentlig-privat samarbejde (OPS)** om udvikling og anvendelse af danske cybersikkerhedsløsninger rettet mod kritisk infrastruktur, bl.a. gennem en mere agil og fleksibel proces i forhold til anskaffelse og indkøb.

2 Styrkelse af cyberforsvaret i danske virksomheder

Danske virksomheder er i stigende grad mål for cyberangreb og -kriminalitet, hvilket også har negative konsekvenser for det danske samfund og vores digitale sammenhængskraft. Mere end halvdelen af de danske virksomheder har været ramt af mindst én sikkerhedshændelse i løbet af de seneste 12 måneder, og analyser viser, at it-sikkerhedsniveauet er for lavt i mere end 40 pct. af de danske SMV'er.

IT-Branchens cybersikkerhedsboard foreslår følgende handlinger:

- **Etablering af et offentlig-privat partnerskab (OPP), der skal varetage opgaven med at indsamle og dele viden** om cybertrusler og -hændelser på tværs af offentlige og private videnkilder og komme med råd og aktuelle anbefalinger, som virksomhederne kan tilgå og agere proaktivt og operationelt på. Suppleret med rådgivning og hjælp til håndtering af sikkerhedshændelser.

- **Målrettet indsats for at hæve minimumssikkerhedsniveauet i SMV'er** med over 10 ansatte, inkl. hjælp til D-mærke certificering (eller en certificering af lignende krav og kvalitet) og tilskyndet via krav om cybersikkerhed, ved offentlige indkøb.

- **Ændret mandat til CFCS der indeholder krav om en øget indsat ift. civilsamfundet**, inkl. veldefinerede krav til CFCS om data- og videnformidling samt klare snitflader og ansvarsfordeling ift. foreslået OPP og øvrige cyberaktører og -myndigheder. Dette fx hjulpet på vej via etablering af en dedikeret privatrettet organisation i CFCS, som det kendes fra England.

- **En effektiv dansk implementering af NIS2-direktivet** bl.a. ved hurtig vedtagelse af relevant lovgivning, så virksomhederne kender rammerne i god tid, etablering af en identisk overordnet rammelovgivning på tværs af sektorer samt klare og konkrete "best-practice"-anbefalinger fra myndighederne, der effektivt hjælper virksomhederne i den rigtige retning og hjælper dem med at ramme det rette niveau af implementering.

3 Øget og accelereret uddannelse af danskere med cybersikkerheds-kompetencer

Ifølge DIGITALEUROPE mangler der 200.000 cybersikkerhedseksperter i Europa. En analyse foretaget af KPMG i samarbejde med Rådet for Digital Sikkerhed estimerer, at Danmark i 2030 mangler mellem 15-20.000 fuldtidsressourcer inden for cyber- og informationssikkerhed. I øjeblikket efterspørger mere end hver tredje danske it-virksomhed medarbejdere med cyberkompetencer. Forsvaret har ligeledes rekrutteringsudfordringer, hvilket besværliggør en nødvendig, digital opgradering. Manglen på kompetencer er generelt en kæmpe hæmsko for cybersikkerheden i Danmark.

IT-Branchens cybersikkerhedsboard foreslår følgende handlinger:

- **Akut investering i uddannelse af flere cyberspecialister** i Danmark, herunder øget optag på it-uddannelser, hvor der er stor efterspørgsel, og hvor kvalificerede ansøgere pt. afvises. Det indebærer øget optag på uddannelser, der er geografisk placeret, hvor de studerende ønsker at bo, og hvor koncentrationen af virksomheder og efterspørgslen efter cyberkompetencer sammenfaldende er størst.

- **Øget integration af viden om cybersikkerhed i relevante (it-)uddannelser.**

- **Øget efteruddannelse** inden for cybersikkerhed herunder anvendelse af korte målrettede erhvervsuddannelser samt fokus på at sikre flere kvalificerede undervisere.

- **Etablering af "IT-sikkerheds-kørekort".** National udrulning af IT-sikkerhedskørekort som skal lære danskerne, hvad det vil sige at være "en digital borger i et digitalt samfund". Baseret på basale regler og basal viden om digitale sårbarheder.

- **Udarbejdelse af plan for styrket uddannelse, rekruttering og fastholdelse af medarbejdere med IT- og cybersikkerhedskompetencer i Forsvaret**, inkl. fx overvejelser om, hvordan man åbner Forsvarets uddannelser mod resten af samfundet og gør dem kompetencegivende – også på IT- og cyberområdet – samt øger optaget af cyberværnepligtige. Der kan også tænkes i generel opkvalificering af danske soldater og officerers IT- og cyberkompetencer, fx som en del af Velkommen Hjem-programmet.

- **Implementering af konkrete tiltag, der skal sikre, at vi tiltrækker, uddanner og fastholder flere internationale studerende og talenter inden for cybersikkerhed**, bl.a. ved at udbyde flere uddannelser på engelsk samt at arbejde for, at de udenlandske studerende på forskellige uddannelsesniveauer kommer i praktik i danske virksomheder og får en større tilknytning til det danske arbejdsmarked og Danmark.

4 Øget digitalisering og cybersikring af det danske forsvar

Måden hvorpå der føres krig har ændret sig drastisk i de senere år, og der er behov for en øget digitalisering og cybersikring af det danske forsvar, så vi bliver bedst muligt rustet mod fjendtlige aktører og stater. Den hastige teknologiske udvikling kræver et betydeligt løft af Forsvarets digitale rygrad og interoperabilitet, hvilket også er en nødvendighed, hvis vi fortsat skal være en relevant samarbejdspartner for vores nære allierede, der i de fleste tilfælde er længere med digitaliseringen af deres forsvar, end vi er i Danmark. Samtidig kan en øget digitalisering bidrage til at imødegå nogle af de mandskabsmæssige udfordringer, Forsvaret forventeligt vil møde, når den danske forsvarsindsats skal udvides.

IT-Branchens cybersikkerhedsboard foreslår følgende handlinger:

- **Nedbringelse af Forsvarets tekniske gæld** (behov identificeret via kasseeftersyn september 2022) – både hvad angår IT-systemer og -infrastruktur forbundet med Forsvarsministeriets overordnede opgaveløsning samt sikrede kommunikationskanaler og anden operativ IT i Forsvaret.

- **Etablering af taskforce til at styrke cybersikkerheden i Forsvarets it-systemer.** Der bør iværksættes en indsats for at sikre, at Forsvarets digitalt baserede kapaciteter er sikre nok. Det gælder alt fra våben- og kommunikationssystemer til administrative systemer og logistiksystemer.

- **Øget investering i offentlig-privat samarbejde (OPS) om udvikling og anvendelse af dansk teknologi og IP** – herunder avanceret software og cybersikkerhed – i det danske forsvar og internationalt. Konkret kunne dette understøttes via:
  - En generelt øget skalering og risiokovillighed ifm. udvikling, integration og certificering af dansk producerede kapaciteter og services.
  - En markant skalering af FMI's medfinansieringsordning samt et udvidet scope af ordningen fra forskning og industriel anvendelse til også at inkludere certificeringer, så danske produkter bliver mere konkurrencedygtige.

- **Øget kapacitet til akkreditering af danske cybersikkerhedsprodukter.** Konkret kunne dette understøttes via:
  - Nedbringelse af den lange sagsbehandlingstid i akkrediterings-sektionen CFCS eller outsourcing af dele af produktakkrediteringerne, fx til danske universiteter.
  - En indsats for at Danmark bliver en Common Criteria "certifikat udstedende nation", således at danske virksomheder og myndigheder ikke skal tilkøbe servicen i udlandet.

- **Øget andel af forsvarsbudgettet brugt på forskning og udvikling mhp. at skabe ny, dansk forsvars- og sikkerhedsteknologi.** Det vil på sigt styrke den danske forsvarsindustri og opbygningen af selvstændige kapabiliteter inden for fx kvanteteknologi, krypteret kommunikation og avanceret cybersikkerhed og gøre Danmark mere uafhængig af udenlandske teknologileverandører, sikre dansk forsyningssikkerhed og skabe nye eksportmuligheder.

Vi skaber et digitalt Danmark med mennesket i centrum

IT-Branchen er Danmarks største brancheorganisation for it- og televirksomheder. Vi hjælper hver dag branchen og samfundet med at vokse.

I IT-Branchen brænder vi for at skabe et digitalt samfund for alle. Et samfund i vækst, og hvor Danmark står som et globalt fyrtårn, fordi vi udnytter teknologien til gavn for klimaet, økonomien og det enkelte menneske. Det gavner Danmark, erhvervslivet, den enkelte borger og vores medlemsvirksomheder.

LÆS MERE OM OS PÅ ITB.DK

IT-BRANCHEN