# IT-Branchens input til National Strategi for Cyber- og Informationssikkerhed

IT-Branchen støtter varmt op om regeringens arbejde med en ny strategi for cyber- og informationssikkerhed.

Det er glædeligt, at regeringen prioriterer indsatsen for bedre cybersikkerhed højt, og at der lægges op til en ambitiøs strategi – det er der også brug for. Det er en reel trussel, som vi i Danmark skal kunne håndtere, og den Nationale Strategi for Cyber- og Informationssikkerhed er et af de væsentligste faktorer i denne sammenhæng.

IT-Branchen er glade for at være inddraget i arbejdet bl.a. gennem Erhvervspartnerskaber for it-sikkerhed, og indirekte gennem regeringens Cybersikkerhedsråd. Vi sætter stor pris på den åbenhed der har været omkring strategien og dens kommissorium. Det har selvstændig værdi, at der fortsat fokuseres på et aktivt, konstruktivt og dialogbaseret samarbejde med branchen.

IT-Branchen har følgende ønsker og forslag til en ny strategi.

#### En national strategi - samarbejde om indsatsen

Den forrige Nationale Strategi for Cyber og Informationssikkerhed fra 2018-2021 har på mange måder været en klar styrkelse af den samlede indsats for bedre sikkerhed, og i særdeleshed samarbejdet på tværs af det offentlige og private. Det ser vi rigtig gerne endnu mere af i en kommende strategi.

Vi kunne godt ønske os, at den nye Nationale Strategi for Cyber og Informationssikkerhed i endnu højere grad bliver en national strategi, som kan samle indsatsen på tværs af både det private, staten, kommuner og regioner. Det ser det ikke ud til at der lægges op til, da kommunerne og Regionerne fortsat ikke synes at være omfattet af strategien. Vi håber at strategien alligevel vil sikre grundlaget for et meget tæt samarbejde om cybersikkerhed på tværs af alle offentlige myndigheder og det private erhvervsliv, og at regeringen vil forankre det tætte offentlige samarbejde om cybersikkerhed andet steds, fx i arbejdet med den Fællesoffentlige Digitaliseringsstrategi.

#### En ambitiøs strategi

Det fremgår af kommissoriet for den nye strategi, at det skal være en ambitiøs strategi. Vi håber, at regeringen vil følge op på dette løfte med nogle ambitiøse initiativer og målsætninger. Med de rette investeringer i cybersikkerhed kan man afløfte store risici. Omkostningen til sikring er lille ift. omkostningen ved oprydning.

En ambitiøs prioritering af cybersikkerhed kan ikke klares indenfor de enkelte ministerier, kommuner og regioners eksisterende økonomiske rammer. Uden den nødvendige finansiering frygter vi, at langt de fleste myndigheder vil søge den laveste fællesnævner.

Samtidig håber vi, at regeringen vil udarbejde en strategi med bindende målsætninger. Strategien bør udpege en række nøgleparametre i forhold til danske myndigheders, virksomheders og borgeres cyber- og informationssikkerhed, og sætte klare mål for at strategien skal forbedre disse. Fx om

* Borgernes og virksomhedernes bevidsthed om opmærksomhed omkring cyber- og informationssikkerhed
* Efterspørgsel og udbud af cybersikkerheds-kompetencer bredt og i dybden
* Virksomhedernes (særligt SMV’ernes) og myndighedernes sikkerhedsniveau
* Omfanget af videndeling, bl.a. gennem indberetninger af sikkerhedshændelser til Center for Cybersikkerhed

Strategien bør ligeledes følges op med jævnlige effektmålinger, der skal vise om indsatsen er lykkedes, og om den har givet den ønskede effekt ift. bedre sikkerhed. Indledningsvist bør der etableres en egentlig cybersikkerheds-baseline.

Endelig er det afgørende, at der skabes gennemsigtighed omkring resultater og konsekvenser af den tidligere og den nye strategi.

#### Videndeling skal understøttes systematisk og effektivt

Vi har brug for at stå sammen i kampen for bedre sikkerhed – derfor er det også godt, at der i kommissoriet lægges op til øget samarbejde – både internt i det offentlige og på tværs af offentligt/privat.

Vi glæder os særligt over, at videndeling om cybersikkerhed er kommet så centralt på agendaen, som det er tilfældet. Vi har rigtig meget viden, der ligger usystematiseret og decentralt. Sidste år fik CFCS fx kun 38 indberetninger om sikkerhedshændelser, hvilket betyder, at meget viden går tabt.

IT-Branchen anbefaler, at der igangsættes en markant offentlig indsats ift. videndeling, hvor det offentlige påtager sig et stort ansvar ift. at understøtte, at alle relevante parter kan, vil og tør dele viden. Fokus skal være bredt på hele Danmark, og ikke kun på kritiske sektorer. Videndeling skal understøttes mere systematisk og effektivt, og det skal være nemt at dele viden, ligesom der skal sikres incitament til at alle deler deres viden. Følgende tre principper kan bane vejen:

* Anonymitet: Det bør være muligt at dele viden om trusler og hændelser i anonym form, eller som minimum med løftet om anonymitet overfor 3. part
* Nemt: Det skal være nemt og ressourcelet at dele viden, og der skal sikres god understøttelse og vejledning i, hvordan og hvad man skal dele
* Incitament: Det skal være tydeligt, at både indberetter og samfundet som helhed har gavn af indberetningerne

Vi foreslår, at der findes offentlige midler til at etablere en ny videndelingsenhed, eller styrke et eller flere af de eksisterende, så følgende initiativer kan løftes:

* Udarbejdelse af udførlige vejledninger til virksomheder og myndigheder, der tydeliggør hvilken viden, der er relevant at dele ,og hvordan og hvor man nemt og hurtigt kan indberette denne viden, herunder vejledning i hvordan viden kan deles med konkurrenter og andre samarbejdspartnere
* Udvikling af digitale løsninger der understøtter anonyme indberetninger af hændelser, herunder afklaring omkring standarder/taksonomier for beskrivelse af sikkerhedshændelser og trusler
* Etablering af en egentlig hændelsesdatabase, hvor viden og data om sikkerhedshændelser kan samkøres
* Systematisk indsamling af viden fra eksisterende aktører, overvågningstjenester og vidensinstitutioner – herunder en selvstændig indsats ift. indsamling af viden andre lande, samt it-sikkerhedsleverandører og producenter
* Bearbejdning af den indsamlede viden om trusler og hændelser, så det aggregeret og anonymiseret kan kommunikeres effektivt og målrettet til borgere, virksomheder og myndigheder
* Konkret tilbagemelding til de virksomheder der indberetter, så de modtager brugbar viden og sammenlignelige data
* Analyser af barrierer for videndeling, herunder juridiske barrierer, samt indsatser for at fjerne disse barrierer

#### Kompetencer er en stor mangelvare

Vi er også glade for at se, at kompetencer og awarenes prioriteres højt i kommissoriet for strategien. Det er et af de områder, hvor vi fortsat er bagud i Danmark. Der uddannes alt for få med cybersikkerhedskompetencer, og cybersikkerhed mangler som fag i mange uddannelser hvor det vil være relevant.

IT-Branchen anbefaler, at regeringen som led i den nye strategi igangsætter initiativer der skal understøtte øget udbud af sikkerhedskompetencer, både it-sikkerhedsspecialister samt generelle it-sikkerhedskompetencer i alle fag.

* Cybersikkerhed bør tænkes tidligt og kontinuerligt ind i uddannelsessystemet. Digital dannelse samt interesse for digital sikkerhed skal skabes tidligt
* Digital sikkerhed bør være et element i alle uddannelser. Det er et grundvilkår for alle medarbejdere
* Skab incitament til at flere prioriterer efteruddannelse indenfor sikkerhed. Manglende cybersikkerhedskompetencer er ikke et generationsproblem

Endvidere bør strategien også indeholde initiativer målrettet kompetenceniveauet i de danske SMV’er. Alt for mange mindre virksomheder har ikke godt nok styr på deres sikkerhed, og mangler kompetencer eller indsigt til at kunne gøre noget ved det. Den kommende strategi bør have et særskilt fokus på at hjælpe SMV’erne, fx gennem

* En central enhed/hotline der kan hjælpe med basal rådgivning og vejledning om it-sikkerhed
* Udbud af kurser målrettet til startups og mindre virksomheder

#### Robusthed og awarenes i befolkningen

Mens kompetencer generelt har et stort fokus i kommissoriet, synes befolkningens sikkerheds-kompetencer at være lidt overset. Borgerne er ”first line of defence”, og en generel indsats ift. borgerens sikkerhedskompetencer bør prioriteres på linje med fx bestyrelser og ledere.

Der er brug for en indsats der hæver bundniveauet i befolkningen ved at satse målrettet på at forbedre befolkningens basale sikkerhedskompetencer, og sikre at borgerne forstår nødvendigheden af cybersikkerhed. Alle danskere har brug for at lære en it-sikkerhedsmæssig bedre adfærd.

Her kan fx hentes inspiration fra PC-kørekortet til at udvikle et værktøj med fokus på sikkerhedskompetencer. Dog er det væsentligt, at værktøjet understøtter løbende læring. It-sikkerhed ikke er en færdighed man kan tillære sig, som fx at køre i bil, men en kultur, der kræver løbende uddannelse og læring.

Et sådant værktøj kan med fordel tilpasses forskellige målgrupper, og der kan tilbydes flere niveauer af læring – fra basal til avanceret. Med inspiration fra fx fødevaresektor kan der ligeledes stilles krav om specifikke niveauer til udvalgte jobs, fx direktører, bestyrelser mv.

#### Stil krav til sikkerheden i myndigheder

Den tidligere strategi opstillede en række minimumskrav til myndigheders arbejde med cyber- og informationssikkerhed, ligesom statslige myndigheder jf. den tidligere strategi er forpligtet til at implementere den internationale sikkerhedsstandard ISO27001.

Dette er en effektiv måde at sikre høj sikkerhed i de offentlige myndigheder, der i høj grad behandler følsomme oplysninger om borgerne. I den nye strategi vil det være oplagt at gå videre med en række yderligere sikkerhedskrav til de offentlige myndigheder, der skal sikre, at sikkerheden styrkes yderligere. Der bør ligeledes følges op på de allerede stillede sikkerhedskrav.

Krav om sikkerhed bør endvidere ikke kun gælde for statslige myndigheder, men i lige så høj grad kommunale og regionale myndigheder og institutioner, der i lige så høj grad håndterer følsomme data. Det kan ligeledes undersøges, om man, i forbindelse med offentlige udbud eller andre sammenhænge, kan pålægge private virksomheder krav om passende it-sikkerhed.

Endelig bør man sikre at alle sikkerhedskrav, risikovurderinger og forholdsregler baserer sig på fakta og på internationale standarder.

#### Styrk internationalt samarbejde

Endelig støtter IT-Branchen varmt op om en prioritering af internationalt samarbejde om cybersikkerhed, og de redskaber og muligheder vi har fx i NATO, FN og EU. Men det vil være stærkt bekymrende hvis Danmark, som det antydes i kommissoriet, skal til at gå i cyber-offensiv mod de aktører, som angriber danske interesser. Hvis Danmark aktivt går ind i cyber-offensiv mod andre aktører, vil det betyde en øget risiko for at danske virksomheder og myndigheder også bliver angrebet, ligesom der er risiko for, at de værktøjer der anvendes spredes til fjendtlige aktører.