IT-Branchens input til national strategi for cyber- og informationssikkerhed (NCIS)

April 2025

IT·BRANCHEN

Hermed følger IT-Branchens initiativforslag til den kommende, nationale strategi for cyber- og informationssikkerhed, der skal træde i kraft fra 1. januar 2026.

IT-Branchen stiller sig naturligvis til rådighed for uddybning og yderligere dialog, fx i regi af vores Policy Board for Cybersikkerhed, der består af en række af Danmarks førende cybersikkerhedsleverandører og -eksperter.

1. En ny NCIS bør hvile på et solidt analysegrundlag og -apparat

➔ IT-Branchen anbefaler, at den kommende NCIS sætter et højt ambitionsniveau med dertilhørende ***bindende målsætninger og løbende status- og effektmålinger*** (modsat den tidligere strategi). Derfor er det også vigtigt, at strategien bygger på et udførligt, analytisk grundlag.

➔ En del af dette analysegrundlag bør omfatte en **risiko- og *sårbarhedsanalyse på samfundsniveau***, hvor vi analyserer den aktuelle sikkerhed og robusthed i den digitale infrastruktur i Danmark og får kortlagt tværsektorielle afhængigheder og konsekvenser af cybersikkerhedsangreb og -hændelser.

Det er vigtigt at understrege, at dette analysearbejde ikke må stå i vejen for en hurtig igangsættelse af de indsatser og initiativer, som skal adressere akutte behov, og som vi allerede ved vil styrke den nationale cyber- og informationssikkerhed. ➔ Derfor bør der også udvikles et mere ***agilt analyseapparat***, hvor man ikke forsøger at analysere alt på én gang, og hvor man samtidig gør det muligt at agere på de analyseindsigter, der opnås undervejs i strategiperioden.

➔ I forlængelse heraf bør man udarbejde en ***"national målestok"*** baseret på internationale standarder og rammeværk, der kan måle effekten af indsatser og indikere, hvor godt eller galt det står til inden for forskellige sektorer og områder, og omdirigere ressourcer efter behov.

➔ Videre er det magtpåliggende, at der følges op på indfrielsen af strategiens målsætninger og tilhørende initiativer med kvalitative/kvantitative mål, og at dette bliver gjort i en ***transparent proces med en tydelig forankring af ansvar for fremdrift***, så der sikres en klar og målbar effekt af de tildelte ressourcer og prioriterede initiativer.

2. Fokus på offentlig-privat samarbejde og udvikling og styrkelse af den danske cybersikkerhedsindustri

Vi skal styrke vores nationale cybersikkerhed i fællesskab. Derfor er det helt afgørende, at en ny NCIS bliver en sammenhængende og samtænkt strategi på tværs af det offentlige, erhvervslivet, civilsamfundet, borgerne og Forsvaret.

Mange af initiativerne i den tidligere NCIS var centreret om det offentliges udvikling af egne enheder, løsninger og tværstatslige videndelingsamarbejder mv. ➔ En ny strategi bør i stedet fokusere mere på et ***styrket offentlig-privat samarbejde***, inkl. nogle klart definerede ambitioner og mål for hvordan ***den danske cybersikkerhedsindustri skal styrkes*** og bidrage til at løfte strategiens målsætninger.

➔ For at understøtte et øget offentlig-privat samarbejde anbefaler IT-Branchen, at der som en del af den nye NCIS ***etableres et formelt samarbejdsforum med en mere systematiseret videndeling, fx af mere omfattende og operationelle trusselsvurderinger, og løbende drøftelser om samarbejder mellem CFCS (nu SAMSIK) og den private cybersikkerheds-branche.***

Forummet skal bl.a. tilsikre, at der skabes klarhed om snitflader, roller og ansvar, så der ydes den bedst mulige vejledning og rådgivning til virksomhederne, inkl. SMV'erne, med bedre udnyttelse af efterretninger, indsigter og ekspertiser på tværs af CFCS (nu SAMSIK) og de private cybersikkerhedsaktører. ➔ Den nye NCIS bør i forbindelse hermed indeholde nogle ***klart beskrevne ambitioner og planer for, hvordan "CFCS" vil åbne mere op*** for videndeling og samarbejde med erhvervslivet som følge af ressortomlægningen af centrets ansvarsområde og kapaciteter fra Forsvarsministeriet til Ministerium for Samfundssikkerhed og Beredskab.

Et eksisterende offentlig-privat samarbejdsforum, som der er god og bred opbakning til, er Cybersikkerhedspagten. Det er dog begrænset, hvad der er leveret af konkrete resultater i Cybersikkerhedspagten, der som forum har potentiale til at kunne spille en langt større rolle ift. at styrke Danmarks cyberforsvar og -beredskab.

Cybersikkerhed er blevet en bredere disciplin over de seneste år. Det handler ikke kun om at skulle forholde sig til tekniske sikkerhedsforanstaltninger. En virksomhed skal ikke kun bekymre sig om målrettede cyberangreb mod egen virksomhed, men også forholde sig til hybride trusler på samfundsniveau, der kan påvirke virksomheden, som fx misinformation, sabotage, destruktive cyberangreb mod kritisk infrastruktur osv. Dertil kan der opstå tvivl og usikkerhed om teknologivalg og -leverandørsikkerhed båret af den geopolitiske ustabilitet og andre faktorer. Det er med andre ord blevet et enormt komplekst trusselsbillede, som virksomhederne skal forholde sig til i deres risikovurdering og beredskab, når vi taler om cybersikkerhed. ➔ De danske virksomheder, inkl. SMV'erne, vil i stigende grad have behov for vejledning til at kunne navigere i dette hybride trusselsbillede, og den opgave kunne passende løses af ***Cybersikkerhedspagten, som via den nye NCIS bør tildeles en mere vejledende og kommunikerende rolle. Dette vil dog kræve, at Cybersikkerhedspagten samtidig tildeles ressourcer til produktion og udbredelse af vejledningsmateriale samt ressourcer til generelt at kunne eksekvere*** på de initiativer, der drøftes mellem de offentlige og de private parter i pagten. Pt. kan pagten betegnes som et idégenerende organ "uden arme og ben" til for alvor at kunne flytte noget mellem pagtens møder – med undtagelse af Varslingstjenesten, som er et konkret produkt af arbejdet i et af pagtens arbejdsspor. Foruden tilgang af ressourcer vil Cybersikkerhedspagtens eksekveringskraft øges, hvis man via den nye NCIS giver pagten mandat til, at de offentlige og private aktører kan rykke tættere sammen og via pagten gå ud at mene og kommunikere noget sammen offentligt. Det kunne fx være ift. at bakke op om D-Mærket.

Herudover er der behov for et ***styrket samarbejde mellem politiet og private sikkerheds-rådgivere***, så vi kan styrke cyberkriminalitetsbekæmpelsen og yde bedre hjælp til virksomhederne efter sikkerhedshændelser. De danske virksomheder efterlades ofte i vildrede og uden tilstrækkelig hjælp efter en sikkerhedshændelse, og alt for få cyberkriminelle bliver retsforfulgt og dømt for deres forbrydelser. Politiet har hverken kompetencerne eller ressourcerne til at ændre på udviklingen. Cyberkriminaliteten har været stærkt stigende over en årrække, og midlerne til at bekæmpe den har slet ikke fulgt med. Derfor skal der allokeres flere ressourcer til området, og det offentlig-private samarbejde skal styrkes. ➔ De private sikkerhedsrådgivere skal i højere grad bringes i spil til at kunne hjælpe med incident response og digital forensics mv. i virksomhederne, fx hjulpet på vej af ***officiel national procedure for hændelseshåndtering med en klar arbejdsdeling mellem offentlige og private aktører, udvikling af procedurer/principper og uddannelse inden for bevissikring samt en certificeret rådgiverliste***, der kan rumme forskellige typer af private sikkerhedsvirksomheder,

inkl. SMV'er, så politiet i højere grad kan fokusere på efterforskningsarbejdet og på at bringe de cyberkriminelle for retten. Der har tidligere været ansats til et sådant initiativ i et samarbejde mellem NC3 og IT-Branchen, men der er behov for politisk vilje og en dedikeret indsats med afsatte ressourcer til for alvor at drive udviklingen videre.

→ Endelig bør strategien generelt have sigte på at ***styrke den danske cybersikkerheds-industris ramme- og konkurrencevilkår***, så vi kan gøre cybersikkerhed til en dansk styrkeposition. Dette kunne fx understøttes vha. øgede investeringer i forskning, udvikling og innovation i nye cybersikkerhedsteknologier, en styrkelse af cybersikkerheden som en del af Danmarks forsvarsindsats (inkl. en øget skalering og risikovillighed ift. udvikling, test, integration, certificering og indkøb af dansk producerede cyberkapaciteter og -services), øget vækstkapital til danske cybersikkerhedsvirksomheder og eksportstøtte. IT-Branchen indgår gerne i en nærmere dialog om, hvordan vi kan udvikle og styrke den danske cybersikkerhedsindustri.

3. Styrket internationalt samarbejde om cybersikkerhed, inkl. i Norden

➔ En ny NCIS bør have fokus på en ***fortsat styrkelse af Danmarks samarbejde om cybersikkerhed med EU***, bl.a. ift. implementering af NIS2 og øvrige cyberregulativer på tværs af EU-medlemslandene, ***samt øget deltagelse i NATO-aktiviteter og -øvelser***.

➔ Herudover anbefaler IT-Branchen, at der – ligesom der er taget initiativ til på forsvarsområdet generelt – særskilt initieres et ***øget samarbejde med vores naboer i de nordiske lande om digital sikkerhed og robusthed***. Et sådant samarbejde kunne omfatte områder som fx fortolkning, harmonisering og implementering af EU-regler; sikkerhedsgodkendelser; datacenterløsninger; fiber- og mobilbeskyttelse og backup; cybertrusselshåndtering og respons; og koordinering af forsyningskæder for kritisk teknologi.

➔ Ift. bekæmpelsen af cyberkriminalitet bør Danmark også være ***mere aktiv i det internationale politisamarbejde*** og udveksling af informationer og erfaringer på tværs af landegrænser i en mere effektiv kamp mod den ofte grænseoverskridende cyberkriminalitet.

4. Styrket cybersikkerhedsniveau i danske virksomheder, særligt i SMV'erne

En ny NCIS bør sætte massivt ind på at hæve cybersikkerhedsniveauet i det brede danske erhvervsliv. Med NIS2 vil der blive stillet skærpede sikkerhedskrav til de større, samfundskritiske virksomheder ➔ Strategien bør derfor tilsikre, at der også fremadrettet ydes ***vejledning og (tilsynsuafhængig) hjælp til virksomhedernes NIS2-regelefterlevelse***.

Men særligt i de danske SMV'er står cybersikkerhedsniveauet ofte ikke mål med virksomhedernes risikoprofiler, så der er behov for øget hjælp, vejledning og rådgivning til dette segment.

➔ IT-Branchen anbefaler, at der med strategien ***etableres et offentlig-privat partnerskab, der har til formål at fremme cybersikkerheden specifikt i SMV'erne*** vha. indsamling og deling af viden, vejledning, udarbejdelse af aktuelle trussels-/risikovurderinger med operationelle anbefalinger, rådgivning og hjælp fra private cybersikkerhedsleverandører til den forebyggende indsats samt håndtering af hændelser. Et arbejde er påbegyndt i regi af Industriens Fond ift. gentænke og revitalisere ambitionen om at etablere en SMV-enhed/"SMV-CERT", som skal løse ovenstående opgave. Det er imidlertid afgørende, at man i en ny NCIS afsætter betydelige offentlige midler og formulerer et forpligtende offentligt engagement til en ny SMV-enhed/"SMV-CERT", der skal løse en alvorlig sikkerhedsmæssig udfordring i dansk erhvervsliv, som ikke alene kan eller bør bero på Industriens Fonds velvilje og investeringslyst.

➔ Herudover bør der etableres en målrettet ***indsats for at hæve minimumssikkerhedsniveauet i SMV'er*** med over 10 ansatte (evt. ansporet af krav til sikkerhed i offentlige indkøb), inkl. fokus på fx implementering af en frivillig NIS2-standard målrettet SMV'er eller hjælp til D-mærkecertificering el.lign. Generelt bør flere SMV'er understøttes i forebyggelse og resiliens med fokus på risikostyring og ledelsesforankring, så foranstaltninger (organisatoriske, tekniske og operationelle) implementeres som risikomitigerende tiltag og ikke blot fra toppen af en simpel tjekliste.

➔ For at beskytte både virksomheder, myndigheder og borgere mod cyberangreb og digital svindel anbefaler IT-Branchen, at strategien indeholder en ***ambition om at fjerne barriererne for udbredelse af tekniske foranstaltninger som fx systematisk DNS-filtrering/-blokering af skadelige domæner***. En mere udbredt DNS-filtrering i Danmark kan med fordel hjælpes på vej via en national, offentlig finansieret indsats for indkøb og tilgængeliggørelse af lister

med skadelige domæner samt tilskyndelse til, at tele- og internetudbyderne tilbyder DNS-beskyttelse som en del af deres tjenester.

➔ Foruden en forebyggende indsats, der skal styrke cybersikkerheden i de danske virksomheder, anbefaler IT-Branchen, at der som en del af NCIS lanceres en ***årlig national cybersikkerhedsøvelse***, hvor både offentlige institutioner og private virksomheder deltager. Formålet er at teste og skærpe aktørernes beredskab, samarbejde og respons på cybertrusler. Initiativet Hele Danmark Øver har vist, at fælles cyberberedskabsøvelser styrker både virksomhedernes og myndighedernes evne til at samarbejde og respondere på angreb, og en ny, årlig, national cybersikkerhedsøvelse kan med fordel bygge på erfaringerne fra Hele Danmark Øver. Cybersikkerhedspagten kunne være initiativtager til øvelsen, så det fælles offentlig-private ejerskab og engagement ift. indsatsen styrkes.

5. Uddannelse og beskyttelse af danske borgere mod digital svindel

De danske borgere rammes i stigende grad af digital svindel. Derfor bør en ny NCIS have fokus på at hjælpe borgerne til bedre at identificere, forstå og undgå digital svindel.

➔ IT-Branchen anbefaler, at der med strategien iværksættes en ***indsats for at hæve det generelle digitale sikkerhedsniveau i befolkningen***. Dette kunne bl.a. ske via en informations- og uddannelseskampagne med national udrulning, hvor lokale aktører, der er tæt på danskernes hverdagsliv, fx skoler, biblioteker, borgerservicecentre, lokale netværk og foreninger, involveres.

➔ Herudover bør strategien også sigte mod at ***øge borgernes opmærksomhed på ny og AI-genereret, digital svindel***. Bevidstheden er lav blandt almindelige danskere, hvad angår hastigheden, hvormed nye former for digital svindel opstår, og hvordan trusselsbilledet skifter blandt andet som følge af udviklingen inden for AI. Vi har brug for langt større fokus på digital svindel, hvordan den rammer den enkelte borger, og hvordan den hele tiden udvikler sig og opdager nye sårbarheder hos både private borgere og virksomheder.

6. Fokus på cybersikkerheden i kritiske, offentlige it-systemer

➔ Selvom NIS2 forventeligt vil hæve cybersikkerheden i de NIS2-omfattede, offentlige enheder, er det vigtigt, at den nye NCIS har fokus på, hvordan vi ***øger investeringsniveauet, der skal afhjælpe den tekniske gæld og dermed højne cybersikkerhedsniveauet i kritiske, offentlige it-systemer***. Dette kan med fordel hjælpes på vej af en (fortrolig) analyse af, hvilke systemer der er mest kritiske og nødstedte, og en efterfølgende plan for hurtig og effektiv opdatering og udbedring.

➔ Derudover vil der fortsat være behov for at ***øge og håndhæve forpligtelsen til at opretholde et højt, ensartet cybersikkerhedsniveau på tværs af stat, regioner og kommuner***. Særligt hvis der, som flere steder antydet, lempes på placering af ansvar og sanktioner i tilfælde af manglende NIS2-regelefterlevelse i kommunerne. Dette bør også være et fokusområde i en ny NCIS.

Eksempelvis bør der stilles krav om, at alle offentlige institutioner har implementeret effektiv DDoS-beskyttelse med klare procedurer for håndtering af angreb.

7. Øget uddannelse og opkvalificering inden for cybersikkerhed

Manglen på kompetencer og kvalificeret arbejdskraft inden for cybersikkerhedsområdet er den største barriere for styrkelsen af Danmarks cyberforsvar og -beredskab. Vi oplever allerede nu et stort udækket behov, og i 2030 vurderes Danmark at mangle op mod 20.000 fuldtids-ressourcer inden for cyber- og informationssikkerhed.

Der er brug for flere cyberspecialister og for at øge udbuddet af cyberkompetencer generelt via uddannelsessystemet.

➔ Derfor anbefaler IT-Branchen, at en ny NCIS indeholder ***en samlet plan for, hvordan optaget på cybersikkerhedsuddannelserne øges, nye uddannelser oprettes og hvordan cybersikkerhed i højere grad integreres i øvrige, relevante (it-)uddannelser***. Dette kræver

naturligvis et tæt samarbejde med særligt Uddannelses- og Forskningsministeriet og uddannelsessektoren generelt.

➔ Lancering af et initiativ som ***Cyber Campus Denmark***, der samler universiteter, myndigheder, Forsvaret, organisationer og virksomheder om forskning, udvikling og uddannelse inden for cyberområdet, vil videre kunne styrke Danmarks konkurrenceevne på cybersikkerhedsområdet og bidrage til at tiltrække internationale cybertalenter og investeringer.

➔ Herudover bør strategien have som ambition at implementere de anbefalinger til ***forbedring af cyberværnepligten***, der er udarbejdet i regi af Cybersikkerhedspagten, inkl. et øget kompetenceniveau blandt de værnepligtige, forlængelse af værnepligten (bl.a. vha. valgfri "grøn tjeneste"), øget samarbejde med uddannelsessystemet og erhvervslivet samt generel skalering af indsatsen.

➔ Endelig anbefaler IT-Branchen, at strategien ser på muligheden for at ***opbygge teknologi- og cyberfokuserede eliteenheder*** i samarbejde med Forsvaret, hvor talentfulde unge inden for eksempelvis matematik og programmering parallelt med eller efter endt civil uddannelse gennemfører et intenst træningsprogram i Forsvaret, der gør dem eksperter i udvikle luftforsvar, operere droner, bygge avanceret cybersikkerhed, bryde koder med hjælp fra AI osv. Disse eliteenheder vil både kunne imødekomme et behov for specialistkompetencer i Forsvaret og det private erhvervsliv, men vil også kunne bidrage til opbygningen af et stærkere tech- og cyberstartupmiljø i Danmark.

I virksomhederne udgør den lange sagsbehandlingstid ift. sikkerhedsgodkendelse af medarbejdere også en kompetenceudfordring, der udfordrer sikkerhedsarbejdet og kan få alvorlige konsekvenser eksempelvis ifm. håndtering af hændelser. ➔ Derfor bør en ny NCIS have som ambition at ***nedsætte sagsbehandlingstiden for sikkerhedsgodkendelser vha. etablering af en platform***, hvor ansøgningsprocesserne er ensartede og fuldt digitaliserede, og hvor godkendelser kan tilgås og gælde på tværs af statslige organer og sektorer.

8. Danmark på forkant med udviklingen inden for nye, kritiske nøgleteknologier

AI er i færd med at ændre cyberkriminalitet, som vi kender den, bl.a. via deepfake, generering af avanceret malware og phishing via mail, sociale medier, telefon og video. Derfor er det helt afgørende, at vi formår at udnytte AI til at øge cybersikkerheden i en højere hastighed end den, hvormed opportunistiske cyberkriminelle tager teknologien til sig og bruger den til at begå cyberangreb og digital svindel.

➔ IT-Branchen anbefaler, at den nye NCIS sikrer et kontinuerligt fokus på udviklingen inden for ny teknologi og afsætter **ressourcer til udvikling af nye AI-drevne cybersikkerheds-løsninger, der kan identificere og forhindre cyberangreb og digital svindel i realtid**.

➔ Samtidig bør ***danske virksomheder understøttes i at få adgang til relevante europæiske samarbejdsprojekter***, eksempelvis via EU Horizon, for at fremme internationalt samarbejde og videndeling. Det bør i den forbindelse også undersøges, hvordan ydelserne i NCC-DK gøres mere relevante og tilgængelige for et bredere udsnit af den danske cybersikkerhedsindustri.

Herudover repræsenterer kvantekryptografi en fremtidssikret teknologi, der kan beskytte følsomme data mod de cybertrusler, der måtte opstå med kvantecomputere. ➔ For at gøre Danmark i stand til at håndtere fremtidige kvantebaserede cybertrusler og opretholde datasikkerhed på højeste niveau, anbefaler IT-Branchen derfor, at en ny NCIS prioriterer ***investeringer i forskning og udvikling af pilotprojekter inden for kvantekryptografi.***

Ovenstående anbefalinger kan med fordel samtænkes og koordineres med udmøntningen af forsvarsforliget og det parallelle behov for at øge andelen af Danmarks forsvarsmidler brugt på forskning og udvikling af forsvarsteknologi. IT-Branchen anbefaler, at yderligere 2 pct. af forsvarsmidlerne prioriteres til forskning og udvikling frem mod 2030. Det vil styrke den danske forsvarsindustri og opbygningen af selvstændige kapabiliteter inden for kritiske nøgleteknologier, inkl. kvanteteknologi, AI, krypteret kommunikation og avanceret cybersikkerhed, og gøre Danmark mere uafhængig af udenlandske teknologileverandører, sikre dansk forsyningssikkerhed og skabe nye eksportmuligheder.