28. januar 2026

Aftale om strategi for cyber- og informationssikkerhed 2026-2029

Der er mellem regeringen og Danmarksdemokraterne, Socialistisk Folkeparti, Liberal Alliance, Det Konservative Folkeparti, Enhedslisten, Dansk Folkeparti, Radikale Venstre, Alternativet og Mike Villa Fonseca (UFG) indgået en aftale vedrørende en ny national strategi for cyber- og informationssikkerhed 2026-2029.

Aftaleparterne er enige om, at Danmark skal stå endnu stærkere i kampen mod cybertruslen. Et vigtigt led heri er en ny strategi for cyber- og informationssikkerhed, der skal bidrage til at styrke cyber- og informationssikkerheden bredt i samfundet.

Aftalepartierne er enige om, at arbejdet med at styrke cyber- og informationssikkerheden i samfundet kræver en vedvarende og fleksibel indsats. Initiativerne i strategien er derfor udarbejdet som rammesættende for en indsats, der muliggør en løbende og dynamisk tilpasning i takt med udviklingen i trusselsbilledet.

Der har siden 2014 været udarbejdet nationale strategier for cyber- og informationssikkerhed i Danmark. Forudsætningerne for den kommende nye strategi er imidlertid forandret. Dette skyldes dels, at den sikkerhedspolitiske situation har forandret sig markant, og dels, at det er første gang, at en national strategi skal udarbejdes på baggrund af NIS 2-direktivet og ny national lovgivning på området.

Danmark står over for det mest alvorlige og komplekse trussels- og risikobillede siden anden verdenskrig. Rusland fører aktuelt hybridkrig mod NATO og Vesten, og det er meget sandsynligt, at den hybride trussel vil stige de kommende år.

Cybertruslen er alvorlig, og danske myndigheder, virksomheder og borgere udsættes dagligt for cyberangreb fra både statslige og ikke-statslige aktører. Angreb kan variere fra forstyrrende overbelastningsangreb til destruktive cyberangreb, som potentielt kan udfordre samfundsvigtige funktioner. Samtidigt rammer cyberkriminelle hele tiden nogen i Danmark med forskellige cyberangreb, fra omfattende ransomware-angreb til tyveri af sensitiv viden og svindel af den enkelte borger.

Dette fremgår af Styrelsen for Samfundssikkerheds årlige trusselsvurdering af cybertruslen mod Danmark, som bl.a. vurderer truslen fra både cyberspoinage og cyberkriminalitet som meget høj. Vurderingen fra 2025 beskriver endvidere de forskellige angrebstyper, f.eks. vurderes det meget sandsynligt, at danske organisationer og borgere vil blive udsat for forsøg på svindel. Den nationale trusselsvurdering suppleres løbende af sektorspecifikke trusselsvurderinger for de enkelte kritiske sektorer.

Grundet den hastige og alvorlige udvikling i trussels- og risikobilledet har regeringen i december 2025 taget initiativ til at prioritere 1 mia. kr. over fire år til etablering af et fælles 24/7-situationscenter i forbindelse med den Nationale Operative Stab. Som led heri skal det nationale værn mod cyberangreb styrkes gennem et dedikeret cyberoperationscenter og opbygningen af et nyt cybermonitoreringsnetværk.

NIS 2-direktivet blev implementeret med NIS 2-loven den 1. juli 2025. Den nye lovgivning betyder, at omfattede myndigheder, herunder kommuner og regioner, og virksomheder i de sektorer, der varetager den kritiske infrastruktur, skal leve op til en række krav til bl.a. cybersikkerhedsforanstaltninger og hændelsesindberetninger, som er underlagt tilsyn og håndhævelsesforanstaltninger i form af bl.a. påbud og bøder. Regeringen har udmøntet 275 mio. kr. årligt fra 2025 og frem til implementeringen af NIS 2-loven. NIS 2-direktivet stiller også krav til nationale strategier, som bl.a. skal adressere områder, der ikke er direkte omfattet af NIS 2-loven, f.eks. borgere og små og mellemstore virksomheder. NIS 2-direktivet har til formål at øge og ensarte cybersikkerhedsniveauet i EU, som en del af den omfattende EU-regulering, der er definerende for arbejdet med cyber- og informationssikkerhed.

Aftaleparterne er enige om, at cyber- og informationssikkerhedsstrategien bygger oven på NIS 2-loven og eksisterende indsatser, og udgør en vigtig del af den samlede indsats på cyberområdet med henblik på at styrke cyber- og informationssikkerheden bredt i hele samfundet.

Aftalens indhold
Der er opstillet fire strategiske pejlemærker for strategien.

Pejlemærke 1. Borgerne har de rette kompetencer til at begå sig sikkert digitalt og beskytte sig mod digital svindel.

Det er vigtigt, at borgerne er informeret om, hvor de kan få hjælp, hvis de bliver ramt af cyberkriminalitet som digital svindel. Der er derfor behov for mere tydelig kommunikation til borgerne herom, ligesom ensartede råd kan styrke forståelsen om digital sikkerhed. Det er ligeledes vigtigt, at myndigheder og private aktører samarbejder om at opsætte relevante foranstaltninger mod digital svindel og igangsætte koordinerede indsatser i takt med, at svindelmetoder udvikles.

For yderligere at styrke og fokusere indsatsen er aftaleparterne enige om følgende initiativer:

- ***Cyberhotline for digital sikkerhed***
  Videreføre og styrke Cyberhotline for digital sikkerhed, der yder forebyggende rådgivning og også kan hjælpe med, hvor borgerne skal rette henvendelse, hvis skaden er sket.

Udbrede kendskabet til Cyberhotlinen og Styrelsen for Samfundssikkerheds øvrige vejledningstilbud til borgerne gennem landsdækkende informationsindsatser med fokus på, at man som borger kan få den rette hjælp og vejledning ét samlet sted i alle faser.

Arbejde for, at flere offentlige såvel som private organisationer aktivt henviser til værktøjerne, så borgerne modtager ensrettet kommunikation om, hvor de kan finde hjælp om digital sikkerhed.

Initiativet vil udbygge Styrelsen for Samfundssikkerheds arbejde med oplysning, rådgivning og konkret hjælp til borgere gennem bl.a. Cyberhotline for digital sikkerhed.

- ***Uddannelse af frivillige i at rådgive gennem "Train-the-trainer"-tilgangen***
  Uddannelse af frivillige, der dagligt møder borgerne, i at rådgive om digital sikkerhed for at styrke rådgivningsindsatsen målrettet f.eks. unge og ældre. Gennem "train-the-trainer"-tilgangen kan rådgivningsindsatsen udbredes til langt flere og blive mere målrettet de enkelte målgrupper.

  Styrelsen for Samfundssikkerhed vil i samarbejde med relevante organisationer uddanne medarbejdere og frivillige, der har daglig kontakt til borgerne, som f.eks. bibliotekarer, medarbejdere på borgerservicecentre, it-frivillige hos Ældresagen, lokalkredse hos IDA, relevante fagpersoner på grundskoler og ungdomsuddannelser mv. i at rådgive andre om digital sikkerhed. For grundskolernes vedkommende kan indsatsen f.eks. indgå som supplement til eksisterende materiale om cyber- og informationssikkerhed.

- ***Nationalt Forum for Bekæmpelse af Digital Svindel***
  Gennem etablering af forummet skabes en strategisk ramme om myndigheder og private aktørers samarbejde om at bekæmpe digital svindel, herunder i takt med, at svindlerne udvikler nye metoder.

  Der afsættes en pulje på 24 mio. kr. i perioden 2026-2029 til løbende tiltag. Derudover afsættes midler til sekretariatsbetjening af forummet. Aftaleparterne vil blive holdt løbende orienteret om udmøntning af puljen.

- ***Nationale råd om digital sikkerhed og retningslinjer for myndigheders digitale kommunikation***
  Der skal udarbejdes nationale råd om digital sikkerhed og retningslinjer for myndigheders digitale kommunikation, så det er tydeligt for borgerne, hvad myndighederne anbefaler. I tillæg hertil skal der udarbejdes fælles retningslinjer for myndigheders digitale kommunikation.

Pejlemærke 2. Virksomheder, med særligt fokus på små og mellemstore virksomheder, har adgang til viden, kompetencer og metoder til håndtering af trusler, der matcher deres risikoprofil.

Danske virksomheder er i høj grad afhængige af hinanden og indgår i værdikæder, der omfatter forskellige brancher, leverandører og virksomhedstyper. Sammenhængene mellem virksomhederne øger risikoen for cyberangreb, der kan sprede sig gennem leverandørkæder. Der er behov for at øge cybersikkerheden i SMV'erne og understøtte en fælles forståelse af, at cybersikkerhed ikke kun er noget, virksomhederne gør for at beskytte sin egen forretning, men også den forretningskæde, virksomheden indgår i.

Det kræver en fælles indsats på tværs af offentlige og private organisationer at løfte cybersikkerheden hos små og mellemstore virksomheder. Der er behov for at højne små og mellemstore virksomheders cybersikkerhedsniveau ved blandt andet at samle og målrette relevante tilbud og værktøjer samt facilitere vidensdeling på tværs af aktører.

Styrelsen for Samfundssikkerhed understøtter allerede i dag de små og mellemstore virksomheders cybersikkerhed gennem viden, vejledning og værktøjer, der f.eks. konkret kan hjælpe med at skabe overblik over virksomhedens systemer og risici, ligesom der også ydes rådgivning gennem Cyberhotlinen for digital sikkerhed.

For yderligere at styrke cybersikkerheden for små og mellemstore virksomheder er aftaleparterne enige om følgende initiativer:

- ***Etablering af SMV-CERT***
  Der etableres en offentlig-privat SMV-CERT (Computer Emergency Response Team), som er en konstruktion kendt fra øvrige sektorer. SMV-CERT skal give de små og mellemstore virksomheder en rolle i cyberøkosystemet og løbende varsle og give adgang til relevant viden og udvikle værktøjer, der matcher virksomhedernes behov.

  Indenfor rammerne af SMV-CERT vil Styrelsen for Samfundssikkerhed arbejde for at udvikle tilbud, der skal gøre det nemmere for de små og mellemstore virksomheder at styrke deres cybersikkerhed. Det vil bl.a. være ved at videreudvikle varslingsordningen, der konkret formidler viden om bl.a. cyberhændelser målrettet små og mellemstore virksomheder, og facilitere lukkede fora til udveksling af viden om cybertruslen for at aktivere den viden, der er i virksomhederne, og sammenholde den med relevante myndigheders viden. Der vil ligeledes være fokus på at udvikle og udbrede eksisterende vejledningstilbud til små og mellemstore virksomheder f.eks. Cyberhotline for digital sikkerhed og at udarbejde nationale råd til de mindste virksomheder.

Ligeledes arbejdes der for, at de små og mellemstore virksomheder får yderligere kendskab til den frivillige, private mærkningsordning D-mærket.

- ***Styrkelse af SMV'ernes cyberberedskab***
  Styrkelse af små og mellemstore virksomheders cyberberedskab gennem beredskabsøvelser og udvikling af konkrete værktøjer hertil.

  Afholde nationale cyberberedskabsøvelser, hvor myndigheder og relevante virksomheder træner alvorlige angrebsscenarier. Arbejdet udføres i samarbejde med Cybersikkerhedspagten, som er et offentligt-privat samarbejde.

Pejlemærke 3. Sikkerhedshændelser i kritisk infrastruktur håndteres effektivt på tværs af sektorer, myndigheder og private aktører i cyberøkosystemet.

I en krisesituation er det essentielt at vide, hvem der gør hvad. Dette gælder både internt i en organisation og på tværs af sektorer og myndigheder. For at kunne reagere effektivt på hændelser, særligt hvis de går på tværs af myndigheder og sektorer, skal der være klarhed over roller og ansvar.

NIS 2-loven stiller bl.a. krav til sikkerhedsniveauet og til hændelsesindberetning i myndigheder og virksomheder i kritiske sektorer, herunder kommuner og regioner. Regeringen har udmøntet 275 mio. kr. årligt fra 2025 og frem til implementeringen af NIS 2-loven. Det er forventningen, at NIS 2-loven og det igangværende arbejde med etablering af tværkommunale it-serviceorganisationer vil bidrage til at øge cybersikkerheden i kommunerne.

Aftaleparterne er enige om vigtigheden af følgende initiativer, der skal styrke det operative samarbejde omkring bl.a. den kritiske infrastruktur:

- ***Cyberoperationscenter og cybermonitoreringsnetværk***
  Regeringen har taget initiativ til etableringen af et dedikeret cyberoperationscenter kombineret med et nyt cybermonitoreringsnetværk i Styrelsen for Samfundssikkerhed. Cybersikkerheden for især myndigheder og virksomheder i den kritiske infrastruktur skal højnes gennem nationalt cybersituationsoverblik og effektivt operativt samarbejde med øvrige aktører på området. På den måde samles monitorering af hændelser, koordination, og krisestyring ét sted. Det skal bidrage til, at cyberhændelser og forsøg på cyberangreb opdages hurtigt mhp. at relevante myndigheder og virksomheder kan blive varslet og reagere med passende foranstaltninger. Der er prioriteret 1 mia. kr. over fire år til det fælles situationscenter, cyberoperationcenteret og cybermonitorieringsnetværket.

- ***Nordisk-baltiske cybersamarbejde***
  Danmark skal stå i spidsen for det nordisk-baltiske cybersamarbejde NBCC (Nordic-Baltic Cybersecurity Consortium), som er støttet af EU med ca. 110 mio. kr. NBCC samler myndigheder fra Danmark, Norge, Island, Finland, Estland, Letland og Litauen og vil få hovedsæde i Danmark. NBCC skal styrke den regionale og nationale cybersikkerhed i den nordisk-baltiske region igennem fælles indkøb af kapaciteter og øget samarbejde.

Aftaleparterne er enige om at supplere indsatsen med følgende initiativ:

- ***Udvikling af nationalt øvelseskoncept***
  Der udvikles nationale øvelseskoncepter, som skal skabe klarhed over roller og ansvar, og der igangsættes nationale, scenariebaserede øvelser.

  Der skal være fokus på at styrke samarbejdet og rollefordeling mellem aktørerne i forskellige myndigheder og sektorer. Dette vedrører særligt snitflader og samarbejder mellem kompetente myndigheder, CERT'er (Computer Emergency Response Teams) i sektorerne, herunder kommuner og regioner, den nationale CSIRT (Computer Security Incident Response Team) samt den Nationale Operative Stab. I den forbindelse skal roller og ansvar på tværs af det digitale og fysiske domæne defineres i forbindelse med håndtering af hændelser. I forhold til kommunerne vil forudsætningerne for det operative samarbejde kunne indtænkes i forbindelse med det igangværende arbejde med etableringen af tværkommunale it-serviceorganisationer.

  Øvelseskoncepterne kan indeholde krisestyringsøvelser, stresstests af operationel robusthed, reetableringstests og tværsektorielle øvelser.

Pejlemærke 4. Cybersikkerhed og kompetencer er en styrkeposition for erhvervslivet

Den stigende efterspørgsel på cybersikkerhedskompetencer er en væsentlig barriere for at opretholde og udvikle Danmarks digitale robusthed. Der er behov for en målrettet indsats for at rekruttere, uddanne og fastholde talenter med relevante tekniske og analytiske kompetencer, der kan bidrage til at styrke beredskab og situationsforståelse på tværs af både offentlige og private aktører.

For yderligere at styrke erhvervslivets styrkepositioner inden for cybersikkerhedsområdet er aftaleparterne enige om følgende initiativ:

- ***Civilt Cyberprogram***

Det er vigtigt at prioritere kompetenceudvikling inden for cybersikkerhed for at imødekomme den stigende efterspørgsel på området. Der etableres derfor et Civilt Cyberprogram i Styrelsen for Samfundsikkerhed for at bidrage til at understøtte bl.a. tidligere cyberværnepligtiges civile karrieremuligheder.

Cyberprogrammet skal fungere som et intensivt opkvalificerings- og træningsforløb målrettet talenter med interesse og potentiale inden for cybersikkerhed, herunder tidligere cyberværnepligtige, ligesom at der vil kigget på mulighederne for, at neurodivergente kan kompetenceudvikle sig via programmet.

Formålet med forløbet er at skabe en struktureret, intensiv og praksisnær indgang til cyberområdet for unge kandidater, typisk med en gymnasial baggrund, som endnu ikke har en videregående uddannelse. Det endelige forløb vil blive udviklet som led i strategien. Aftaleparterne vil løbende blive holdt orienteret om programmets udvikling.

Aftaleparterne noterer sig, at initiativet supplerer følgende igangsatte initiativer:

- ***Styrket forsknings- og innovationsindsats inden for bl.a. cybersikkerhed***
  For at understøtte forskning og erhvervsliv er der prioriteret ca. 2,9 mia. kr. i 2026-2029, som beskrevet i *Aftaler om Forskning og Innovation 2026-2029*, hvori der prioriteres en styrket forsknings- og innovationsindsats inden for kritiske og digitale teknologier, kvanteteknologi og forsvarsforskning, som kan bidrage til bl.a. styrket cybersikkerhed i forhold til intensiveret dataanvendelse, sikker datadeling og kommunikation, kryptografi, softwareudvikling, menneskelig adfærd samt beskyttelse af kritiske teknologier med dual-use potentiale.

- ***Styrket teknologisk service til virksomheder gennem Godkendte Teknologiske Serviceinstitutter***
  Der ydes styrket teknologisk service til virksomheder gennem Godkendte Teknologiske Serviceinstitutter (GTS'er), herunder gennem udvikling og test af nye produkter og tjenester, som beskrevet i resultatkontrakter mellem GTS'erne og Uddannelses- og Forskningsministeriet for perioden 2025-2028.

- ***Nye videregående uddannelser inden for cybersikkerhed***
  Der er i de seneste år godkendt en række nye videregående uddannelser og specialiseringer inden for cybersikkerhed og it. Det gælder både ordinære videregående uddannelser som bl.a. akademiske bacheloruddannelser, kandidatuddannelser og professionsbacheloruddannelser, der har betydning

for, hvor mange dimittender, der i fremtiden kommer ud på arbejdsmarkedet med kvalifikationer og viden på cyberområdet, ligesom der er godkendt nye udbud på efter- og videreuddannelsesområdet, som giver mulighed for, at personer, der allerede er i arbejdsstyrken, kan opkvalificere sig og tilegne sig nye kompetencer inden for cybersikkerhed.

- ***Styrket Cyberværnepligt***
  Aftaleparterne bag Anden delaftale under Forsvarsforliget 2024-2033 har aftalt at følge udviklingen på cyberområdet tæt med henblik på at kunne styrke cyberværnepligten, herunder i forhold til varighed og antallet af værnepligtige i forhold til Forsvarets og det civile samfunds behov. Konkret udvides cyberværnepligten fra 10 til 11 måneder og fra ca. 30 til aktuelt ca. 60 værnepligtige årligt.

Aftalens karakter
Aftalen har karakter af en stemmeaftale, der opfylder forudsætningen om, at der er et simpelt flertal af mandater i Folketinget, og aftalepartierne enige om at stemme for den lovgivning, der er nødvendig for at udmønte denne aftale.

Økonomi
Aftaleparterne er enige om at afsætte 211 mio. kr. i 2026-2029 og 33 mio. kr. årligt i 2030 og frem til initiativerne med denne aftale*, jf. tabel 1*. Aftalen finansieres af reserven til styrket samfundssikkerhed og beredskab, der er opført på finansloven for 2026.

Det svarer til 52,5 mio. kr. i 2026 faldende til 52 mio. kr. i 2029, der omfatter 27,5 mio. kr. i 2026 faldende til 27 mio. kr. i 2029 til nye initiativer på cyberområdet og 25 mio. kr. årligt til strategiens bemandingsmæssige fundament, som er en delvis videreførelse af de samlede bemandingsressourcer fra den seneste strategi fra 2022-2024. De pågældende medarbejdere udfører i dag opgavevaretagelsen på cyberområdet i Styrelsen for Samfundssikkerhed, og vil fremadrettet skulle understøtte, implementere og udføre strategiens initiativer, som primært indeholder driftsmidler.

Tabel 1
Økonomi i aftalen

Mio. kr., 2026-pl	2026	2027	2028	2029	I alt 2026-2029	Årlige udgifter i 2030 og frem
Udgifter	**52,5**	**54,5**	**52,0**	**52,0**	**211,0**	**33,0**
Bemandingsmæssigt fundament for cyberindsatsen	25,0	25,0	25,0	25,0	100,0	25,0
Nye initiativer på cyberområdet	27,5	29,5	27,0	27,0	111,0	8,0
Heraf pulje til forum	*6,0*	*6,0*	*6,0*	*6,0*	*24,0*	-
Finansiering	**52,5**	**54,5**	**52,0**	**52,0**	**211,0**	**33,0**
Reserve til styrket samfundssikkerhed og beredskab	52,5	54,5	52,0	52,0	211,0	33,0