Bilag 1

12. december 2016

Kommissorium for det tværministerielle arbejde med den nationale strategi for cyber- og informationssikkerhed 2017-2019.

Indledning

Det fremgår af regeringsgrundlaget "For et friere, rigere og mere trygt Danmark", at regeringen vil igangsætte arbejdet med en ny strategi for cyber- og informationssikkerhed, som skal gøre danske myndigheder og private aktører inden for centrale sektorer parate til at beskytte den danske digitale infrastruktur.

Udgangspunktet for arbejdet med udarbejdelse af en ny strategi for cyber- og informationssikkerhed er, at der bygges videre på de indhøstede erfaringer. I december 2014 blev den første nationale strategi for cyber- og informationssikkerhed lanceret. Strategiens væsentligste overordnede resultat var en modning af dialogen om cyber- og informationssikkerhed og digital risikoledelse hos de berørte parter. Dette fundament skal udnyttes i den kommende strategi til at skabe et endnu stærkere fundament for den nationale cyber- og informationssikkerhed.

Baggrund

Baggrunden for en ny national cyber- og informationssikkerhedsstrategi er den stadigt mere omfattende digitalisering. Udviklingen giver store muligheder for Danmark og er en forudsætning for den fortsatte udvikling af velfærdssamfundet. Men med digitaliseringen følger også nye sårbarheder. Udfordringen med at sikre samfundets robusthed og sikkerhed med hensyn til både informationssikkerhed og opretholdelsen af samfundsvigtige funktioner vokser. Det gælder bl.a. i forhold til hacker- og virusangreb, systemnedbrud, medarbejderes tilsigtede og utilsigtede brud på cyber- og informationssikkerheden samt kompromittering af personlige oplysninger.

Den betydelige stigning i datamængderne stiller øgede krav til beskyttelsen heraf. Samtidig har et skærpet trusselsbillede store konsekvenser for den nationale sikkerhed, idet truslen fra cyberspionage mod danske myndigheder er meget høj, og cyberoperationer integreres i stadigt flere landes potentielle magtanvendelse. Endvidere har kriminelle adgang til avancerede teknikker, og der er på længere sigt risiko for, at det også vil lykkes for terrornetværk at opbygge cyberangrebskapacitet.

Opretholdelsen af systemer og tjenester, som myndigheder, borgere og virksomheder kan have tillid til, er en forudsætning for den videre udvikling af velfærdssamfundet og udnyttelsen af de digitale muligheder. Trusler mod informationssikkerheden er reelle og har afledte effekter som eksempelvis økonomisk tab og tab af tillid til såvel den digitale udvikling som til de aktører, der udøver samfundsvigtige funktioner. Sikkerhed i løsningerne skal kontinuerligt afvejes i forhold til omkostninger, brugervenlighed og effektivitet.

I det kommende EU-direktiv om net- og informationssikkerhed (NIS) fastlægges forpligtelser

for alle medlemsstater til at gennemføre en række tiltag med sigte på at opretholde sikkerheden i net- og informationssystemer, herunder en forpligtelse for medlemsstaterne til at vedtage en national strategi på området. Den nye danske cyber- og informationssikkerhedsstrategi vil kunne bidrage til efterlevelse af denne forpligtelse, ligesom initiativer med henblik på koordination af den danske implementering af direktivet vil kunne indgå i strategien.

Udgangspunktet
Tilgangen til arbejdet med den nye strategi bygger på følgende forudsætninger:

- Truslerne på cyber- og informationssikkerhedsområdet påvirker på tværs af sektorer og retter sig mod både borgere, myndigheder og virksomheder. De systemer, som understøtter kritiske funktioner i samfundet, er ofte sammenhængende og gensidigt afhængige.

- En række sektorer, der varetager samfundskritiske funktioner, kræver målrettede og tilpassede tiltag.

- Afvejning af sikkerhed, brugervenlighed og effektivitet.

Ud over en særskilt behandling af en række udvalgte sektorer skal der være fokus på en styrkelse af informations- og erfaringsudveksling om trusler og sikringsforanstaltninger på tværs. Udgangspunktet for strategien er, at den kan understøtte tværgående udveksling og koordinering, og at myndighederne og virksomhederne er ansvarlige for sikkerheden på eget område, jf. sektoransvarsprincippet.

De deltagende ministerier er således ansvarlige for gennemførelse af strategien inden for eget ressortområde, men samtidig bør samtænkning af løsninger på tværs af sektorerne vægtes. I den forbindelse skal arbejdsgruppen vurdere, om sektoransvarsprincippet kan opretholdes i alle tilfælde, da imødegåelsen af visse cybertrusler kræver en meget specialiseret viden, kapacitet og et tværgående samarbejde.

Mål for arbejdet
Strategien bør sætte klare mål for Danmarks nationale cyber- og informationssikkerhed, idet der skal tages højde for:

- den fortsatte digitalisering af samfundet og de forbundne fordele og risici,
- balancen mellem sikkerhed, brugervenlighed og effektivitet,
- trusselbilledet på området,
- arbejdet i lande, Danmark normalt sammenligner sig med.

Den gensidige afhængighed og sårbarhed nødvendiggør en øget tværsektoriel tilgang til håndtering af trusselsbilledet samt et øget behov for informations- og erfaringsudveksling om trusler og sikringsforanstaltninger på tværs af sektorerne i forhold til cyberangreb og informationssikkerhed. Strategien skal øge det kollektive vidensniveau, den fælles robusthed og evnen til at forebygge og reagere, blandt andet gennem klar arbejdsdeling og bedre netværk på

tværs af myndigheder og sektorer. Herunder skal strategien have fokus på en udbygget beskyttelse imod avancerede angrebsteknikker, fortsat modning af viden om cyber- og informationssikkerhed og digital risikoledelse i danske virksomheder og myndigheder samt fælles tekniske og organisatoriske foranstaltninger.

I den første strategi var der særligt fokus på det statslige område, telesektoren og energisektoren. Ligeledes fremgik det af strategien, at det ville blive vurderet, om der var behov for at inddrage andre sektorer, fx finanssektoren, i en kommende strategi. Fsva. finanssektoren er der oprettet et samarbejdsforum mellem myndigheder og vigtige aktører i den finansielle sektor - Finansielt Sektorforum for Operationel Robusthed - som har til formål at øge den operationelle robusthed ved it-anvendelse herunder robustheden over for cyberangreb. Initiativer på det finansielle område vil tage udgangspunkt i det arbejde, der er igangsat.

Strategien skal have fokus på sektorer, der varetager afgørende samfundskritiske funktioner, der med det nuværende trusselsbillede er behov for at sætte særligt ind over for. Med udgangspunkt i målet om at udarbejde en strategi, der dels har en række tværgående indsatser, dels adresserer en række udvalgte centrale sektorer, kan den kommende strategi have fokus på følgende:

- Energisektoren
- Telesektoren
- Transportsektoren
- Finanssektoren
- Sundhedssektoren
- Statslige myndigheder og institutioner, der varetager samfundskritiske funktioner.

De deltagende ministerier skal ud fra en risikovurdering på eget område særligt forholde sig til sikring af systemer og national infrastruktur, som understøtter væsentlige funktioner i samfundet, og bl.a. indtænke samarbejdet med private it-driftsleverandører af offentlige løsninger og adgangen til fællesoffentlige systemer.

Ministerierne skal med udgangspunkt i det aktuelle trusselsbillede udvikle relevante initiativer til håndtering af risici såvel inden for eget ressort som af tværgående karakter. Initiativer skal baseres på en afvejning mellem den vurderede trussel, kritikalitet og sårbarhed, forretningsmæssige hensyn, brugervenlighed og økonomi, herunder omkostninger ved ikke at gøre noget.

Initiativerne i strategien forventes bl.a. at have fokus på:

- Kompetencer, kapacitet og viden inden for cyber- og informationssikkerhed, herunder om trusselsbilledet i Danmark.
- Regulering, herunder både national og international, fx implementeringen af NIS-direktivet og databeskyttelsespakken.
- Internationalt samarbejde om cyber- og informationssikkerhedsindsatsen.

Arbejdet skal munde ud i en kortfattet national strategi for cyber- og informationssikkerhed, indeholdende strategiske mål og konkrete initiativer inden for de nævnte sektorer og indsatsområder.

I arbejdet med strategien skal der tages højde for, at der allerede foreligger en fællesoffentlig digitaliseringsstrategi, som indeholder en række initiativer for at styrke informationssikkerheden i offentlige myndigheder, og at regeringen har nedsat et Virksomhedsråd for IT-sikkerhed, der skal komme med anbefalinger primo 2017 til en styrkelse af it-sikkerhed og ansvarlig datahåndtering i særligt små og mellemstore virksomheder.

Tidsplan og organisering
Et udkast til strategien, herunder eventuelle økonomiske konsekvenser, skal forelægges regeringen inden udgangen af maj 2017. Strategien udformes for en periode på tre år (2017-2019) med strategiske målsætninger, konkrete initiativer og angivelse af milepæle for hvert år. Der skal i strategien indgå en beskrivelse af, hvordan der vil ske afrapportering til regeringen på gennemførelse af initiativerne.

Halvvejs i strategiperioden rapporteres en status for arbejdet med initiativerne i relation til den strategiske målsætning til regeringen. I den forbindelse vil kunne indgå forslag til eventuelle yderligere initiativer i strategiperioden, herunder initiativer formuleret med deltagelse af de fagansvarlige ministerier med sigte på at opfylde NIS-direktivets krav.

Den eksisterende tværministerielle arbejdsgruppe med deltagelse af Forsvarsministeriet, Udenrigsministeriet, Justitsministeriet, Finansministeriet, Erhvervsministeriet, Uddannelses- og Forskningsministeriet, Energi-, Forsynings- og Klimaministeriet samt Skatteministeriet udvides som følge af de tilføjede sektorer med Sundheds- og Ældreministeriet og Transport-, Bygnings- og Boligministeriet. Arbejdsgruppen kan vælge at invitere andre ministerier til at deltage på ad hoc-basis, såfremt gruppen vurderer det relevant.

Formandskabet for arbejdsgruppen varetages af Forsvarsministeriet, mens Center for Cybersikkerhed, Erhvervsministeriet/Erhvervsstyrelsen, Politiets Efterretningstjeneste og Digitaliseringsstyrelsen i fællesskab varetager sekretariatsfunktionen.

Arbejdsgruppen skal aktivt søge dialog med relevante aktører, herunder eksempelvis brancheorganisationer, med henblik på at indhente bidrag til arbejdet.

Økonomi
Omkostninger til myndighedernes initiativer og handlingsplaner i forlængelse af strategien afholdes som udgangspunkt inden for egne rammer.

Omkostninger til udgivelse af strategien afholdes af Digitaliseringsstyrelsen og Center for Cybersikkerhed i fællesskab.