

Bilag 1

Kommissorium for udarbejdelse af en ny national strategi for cyber- og informations-sikkerhed

Indledning

Danmark er et af verdens mest digitaliserede lande. Digitale løsninger er helt centrale for driften af samfundsvigtige funktioner og for størstedelen af dansk erhvervsliv. Digitaliseringen udvikler velfærdssamfundet, men gør det samtidig sårbart. Digitaliseringen og den teknologiske udvikling giver mange muligheder, men medfører også en fortsat forandring af trussels- og risikobilledet. Jo flere digitale systemer, vi anvender og kobler sammen, jo flere steder kan vi blive angrebet.

Cybertruslen er blandt de mest alvorlige trusler mod Danmark og danske interesser, jævnfør Center for Cybersikkerheds trusselsvurdering. Cyberangreb kan i værste fald medføre, at samfundet ikke kan fungere. Danmark rammes dagligt af cyberangreb, og den høje cybertrussel er blevet et grundvilkår.

Kriminelle stjæler fra danske borgere og virksomheder via internettet, og statslige aktører udfører politisk og kommercielt motiveret spionage mod virksomheder og danske myndigheder, herunder danske repræsentationer i udlandet. Truslen mod cyber- og informationssikkerheden rammer bredt, og de digitale virkemidler skal således ses i samspil med aktøernes øvrige metoder. Spionage og cyberangreb vil kunne få alvorlige økonomiske konsekvenser og påvirke dansk sikkerhed og velfærd negativt. I værste fald kan destruktive cyberangreb få omfattende konsekvenser for samfundsvigtige funktioner.

Cyberkriminelle udfører oftest relativt simple angreb mod mange potentielle ofre på én gang i håbet om at få et afkast fra så mange som muligt. Det sker typisk gennem phishing-angreb eller inficering af hjemmesider med malware. Disse angreb udgør en vedvarende trussel for virksomheder, myndigheder og borgere i Danmark.

Der er en stigende trussel fra målrettede ransomware-angreb. Kriminelle forsøger at afpresse myndigheder og virksomheder for store beløb ved at kryptere centrale dele af offerets it-systemer. Som led i en række separate angreb på danske virksomheder blev eksempelvis virksomheden Demant udsat for et ransomware-angreb i efteråret 2019, der ifølge virksomheden medførte et tab på op mod 650 mio. kr.

Viden og awareness om trusler mod cyber- og informationssikkerheden er stadig ikke tilstrækkeligt udbredt. Det betyder bl.a., at medarbejdere kan være sårbare overfor spionage og uforvarende dele beskyttelsesværdige informationer, og at hackerne fortsat kan misbruge gammelkendte sårbarheder, så selv simple cyberangreb kan have alvorlige konsekvenser.

Danmark skal være digitalt sikkert

Danmark skal være digitalt sikkert. Danskerne skal være trygge ved digitale løsninger og vide, hvordan man beskytter sig og færdes sikkert digitalt. Virksomheder og myndigheder skal have et stærkt og vedvarende fokus på cyber- og informationssikkerheden, så brugere og

samarbejdspartnere bevarer tilliden til de ydelser, der leveres. Arbejdet med cyber- og informationssikkerhed skal fortsat tage udgangspunkt i en risikobaseret tilgang, hvor ressourcerne til sikkerhedstiltag målrettes de mest kritiske data og systemer.

En stærk sikkerhed fordrer, at cyber- og informationssikkerhed prioriteres ledelsesmæssigt, både hvad angår forståelse for truslerne, medarbejder-awareness og sikkerhedskultur, men også de tekniske sikkerhedsforanstaltninger. Ledelser og bestyrelser bør bl.a. forholde sig proaktivt til organisationens risikovurderinger, og beslutte, hvilke sikkerhedstiltag, der bør gennemføres.

Endvidere er det afgørende, at det gode samarbejde på tværs af myndigheder og virksomheder styrkes, så videndeling og fælles løsninger tænkes ind, hvor det er relevant samt understøttes af højt specialiseret rådgivning fra central hold. Behovet for samarbejde gælder også på internationalt plan, hvor Danmarks indsats skal bidrage til at skabe et åbent, sikkert og troværdigt internet, og beskytte de samfundsvigtige digitale infrastrukturer.

Kernefunktioner i Danmark skal være robuste og modstandsdygtige, og de skal kunne videreføres, også selvom de primære digitale funktioner sættes ud af kraft i kortere eller længere tid.

En videreførelse af vigtige samfundsfunktioner ved en omfattende cyberhændelse og forstyrrelse forudsætter, at der bl.a. er taget stilling til digital redundans og forsyningssikkerhed. På samme vis skal et styrket fokus på krisehåndtering og resiliens i dansk erhvervsliv afbøde de økonomiske omkostninger, som en omfattende cyberhændelse vil få for det danske samfund. Der er således behov for at sikre den nødvendige teknologianvendelse og kompetencer, som bør være et fundament for hele samfundet. Indsatser i det digitale domæne skal bl.a. designes med blik for de afledte konsekvenser i det fysiske domæne, og samfundsvigtige funktioner skal være beskyttet, så økonomien og samfundet ikke rammes af større forstyrrelser.

På denne baggrund skal der udarbejdes en ny national cyber- og informationssikkerhedsstrategi, der bygger videre på indsatser og erfaringer fra den nuværende strategi, og som tager udgangspunkt i behovet for at styrke den digitale robusthed og resiliens på tværs af samfundet. Som led i den indeværende cyber- og informationssikkerhedsstrategi er der udarbejdet en status for arbejdet med cyber- og informationssikkerhed (tilstandsanalyse) samt udfordringer på tværs af myndigheder, samfundskritiske sektorer, virksomheder og borgere, *jf. nedenfor*.

Status for arbejdet med cyber- og informationssikkerhed (tilstandsanalyse)

Bevidstheden om cyber- og informationssikkerhed er generelt stigende i Danmark, herunder hos de statslige myndigheder. Det skyldes bl.a. en række statslige indsatser, herunder de decentrale sektorstrategier for cyber- og informationssikkerhed og krav om ISO 27001-implementering.

Der udestår dog fortsat et arbejde med at få ledelsen i alle statslige myndigheder til at prioritere implementeringen af sikkerhedsstandarder, ligesom arbejdet med risikostyring- og vurderinger kan forankres dybere. Dertil kommer, at der i Danmark generelt er mangel på relevante kompetencer og en manglende brug af tekniske foranstaltninger, herunder særligt blandt visse SMV'er og yngre danskere.

For yderligere uddybning henvises til resume af tilstandsanalyse for cyber- og informationssikkerhedssituationen i Danmark (bilag 2).

Formål

Den hidtidige indsats for et højt cyber- og informationssikkerhedsniveau har øget modenheten på tværs af samfundet, men det er nødvendigt, at ambitionsniveau og fokusområder følger med den løbende udvikling i trusler og sårbarheder.

Der lægges op til en ambitiøs strategi, der bygges op om fire centrale temaer: *For det første* skal det indtænkes, hvordan den forebyggende indsats mod sikkerhedshændelser kan skærpes ved at sikre en vedvarende topledelsesmæssig forståelse, forankring og prioritering af cyber- og informationssikkerhed, samt en større videns- og awarenessindsats rettet mod ledere og medarbejdere i statslige myndigheder og virksomheder, også ift. de tekniske tiltag. Konkret for lederne skal der ses på tiltag, der vedvarende kan bibringe dem viden og redskaber til deres prioritering af cyber- og informationssikkerhed.

For det andet indtænkes, hvordan samfundet er forberedt på at opretholde vigtige samfundsfunktioner og økonomisk aktivitet i en krisesituation, hvor Danmark rammes på helt centrale digitale funktioner. Dette kræver bl.a., at der er overblik over kernefunktioner og ikke mindst "single-point-of-failures", der kan understøttes af en central indsats.

For det tredje indtænkes, hvordan videndeling, information og samarbejde på tværs af virksomheder, sektormyndigheder og myndigheder med tværgående ansvar kan styrkes.

For det fjerde indtænkes hvordan man gennem en styrket internationalt samarbejde kan øge omkostningerne for kriminelle og statslige aktører, der udfører cyberangreb mod Danmark, ved i højere grad at påføre konsekvenser for dem, der angriber Danmark i cyberspace.

Strategien skal udvides i bredden ved at omfatte yderligere sektorer, der skal udvikle sektorstrategier. Det kan i den forbindelse vurderes, hvilket behov for central understøttelse sektorerne vil have i udviklingen og implementeringen af strategierne. Det kan overvejes, om der kan etableres en mellemkategori af sektorer, der ikke er samfundskritiske som helhed, men som har digitale løsninger (f.eks. på undervisningsområdet), der i en krisesituation kan skifte karakter fra supplerende infrastruktur til kritisk infrastruktur.

I dybden skal ambitionerne øges, både i sektorenes indsats og i forhold til de tværgående indsats, så den generelle robusthed og modstandsdygtighed styrkes, blandt danske virksomheder, borgere og myndigheder. For statslige myndigheder vil det blive et fokuspunkt, hvordan en dybere implementering af *best practice* og krav kan sikres, fx gennem en styrket opfølgings- og vejledningsindsats eller gennem eksempelvis en udvidelse af de eksisterende 20 tekniske minimumskrav til statslige myndigheder, der er blevet obligatoriske i indeværende strategi-periode. Et væsentligt fokus vil være, hvordan efterlevelse af god sikkerhedsadfærd i højere grad kan understøttes af en højt specialiseret central rådgivningskapacitet, hvori der kan opbygges kapacitet til at yde situationsbestemte råd og vejledning i spørgsmål om cyber- og informationssikkerhed, eksempelvis i form af etablering af en cyberhotline. I den forbindelse er det afgørende, at kompetencerne på it-sikkerhedsområdet anvendes effektivt og hensigtsmæssigt, så der undgås dobbeltfunktioner, og så vejledningsindsatsen målrettes derhen, hvor der er mest brug for den.

Som led i det forberedende strategiarbejde udarbejdes desuden et overblik over myndighedernes nuværende ansvarsområder og opgaveløsning relateret til cyber- og informationssikkerhed i staten samt omkostningerne forbundet hermed.

Forudsætningen for myndighedssamarbejdet vil fortsat være sektoransvarsprincippet, bl.a. i tilfælde af en krisesituation, hvor myndigheder med ansvar for den daglige drift også har ansvar for cyber- og informationssikkerheden, understøttet af ambitiøse centrale initiativer. Arbejdet med at implementere de nuværende sektorstrategier fortsættes i 2020-21 og eventuelle yderligere indsats, som følge af den nye nationale strategi, bygger på dette arbejde. Hertil kan der samarbejdes på tværs af sektorerne om fælles løsninger til gavn for virksomheder, myndigheder og borgere.

Opbygning, organisering og tidsplan for arbejdet

Den nye strategi bygges op om en fire overordnede temaer:

- Ledelsesforankring og kompetenceopbygning, herunder f.eks.:
 - Styrket indsats i forhold til viden, awareness og adfærd for både ledere og medarbejdere på statslige arbejdspladser, blandt virksomheder og borgere
 - Styrket indsats på uddannelsesområdet
- Robusthed og resiliens, herunder f.eks.:
 - Styrket indsats i både staten og i de samfundskritiske sektorer
 - Styrket fokus på efterforskning af cyberangreb og spionage
 - Styrket indsats i erhvervslivet med særligt fokus på SMV'er
 - Styrket fokus på sikkerhed i nye teknologier
- Samarbejde og organisering, herunder f.eks.:
 - Styrket central kapacitet til at håndtere cyber- og informationssikkerhedsudfordringer
 - Styrket samarbejde på tværs af forskning, erhvervsliv og den offentlige sektor inden for cyber- og informationssikkerhed

- International indsats og bidrag, herunder f.eks.:
 - Styrket internationalt samarbejde for at øge omkostninger for såvel kriminelle som statslige aktører, der gennemfører cyberangreb mod Danmark eller vores nære allierede
 - Styrket dansk profil i FN, EU, NATO og blandt ligesindede lande

Arbejdet skal munde ud i en ambitiøs national strategi for cyber- og informationssikkerhed, der indeholder konkrete initiativer, der adresserer udfordringerne og understøtter de strategiske pejlemærker.

Arbejdet udføres i regi af den eksisterende styregruppe for den nationale strategi for cyber- og informationssikkerhed. For at sikre bred inddragelse og forankring af strategiens initiativer inviteres alle ministerområder til at deltage i styregruppen ifm. udarbejdelse af strategien. Formandskabet for styregruppen varetages af Finansministeriet (Digitaliseringsstyrelsen) og Forsvarsministeriet (Center for Cybersikkerhed). Styregruppen sekretariatsbetjenes af Finansministeriet/Digitaliseringsstyrelsen, Forsvarsministeriet/Center for Cybersikkerhed, Erhvervsministeriet/Erhvervsstyrelsen og Justitsministeriet/PET.

Cybersikkerhedsrådet og Erhvervspartnerskabet for øget IT-sikkerhed bliver inddraget med henblik på at levere input til strategiens overordnede temaer og eventuelt indspil til specifikke initiativer. Endelig vil styregruppen løbende inddrage en bredere kreds af relevante interessenter.

Regeringen forelægges et udkast til strategi 1. kvartal 2021. Som led i udarbejdelsen af strategien forelægges regeringen i ultimo 2020 en status på arbejdet, hvori der redegøres for ambitions- og udgiftsniveauet forbundet med de foreløbige udkast til initiativer. Der anvises i den forbindelse modeller for, hvordan strategien kan tilpasses forskellige ambitionsniveauer.