REGERINGEN

National strategi for cyber- og informationssikkerhed

Finansministeriet

MAJ 2018

Indhold

Forord

I Danmark oplever vi i disse år ligesom resten af verden, at den teknologiske udvikling går hurtigere og hurtigere, at vi i stigende grad forbindes via digitale løsninger, og at vi alle – myndigheder, virksomheder og borgere – bliver stadigt mere afhængige af internettet, og de muligheder det bringer.

Danmark er et af de mest digitaliserede lande i verden, og digitaliseringen er et afgørende middel både for udviklingen af den offentlige sektor og for private virksomheders vækst og konkurrenceevne.

Som danskere er vi vant til at interagere både med virksomheder og offentlige myndigheder gennem digitale løsninger, og vi har en grundlæggende tillid til, at udvekslingen af data og informationer sker på en ansvarlig og sikker måde med respekt for den enkeltes privatliv.

Tilliden til sikkerheden i digitale løsninger er afgørende for den fortsatte digitale udvikling af vores samfund. Vi skal beskytte vores data og sikre, at de digitale løsninger, vores velfærdssamfund er afhængigt af, er beskyttet mod ødelæggende angreb udefra.

Regeringen øger nu ambitionsniveauet for indsatsen på cyber- og informationssikkerhedsområdet og vil i de kommende år investere 1,5 mia. kr. i Danmarks cyber- og informationssikkerhed.

Regeringen og forligspartierne har med Forsvarsforliget 2018-2023 styrket beskyttelsen af Danmark mod cybertrusler markant. Nu styrkes arbejdet yderligere med en ny national strategi for cyber- og informationssikkerhed, der binder den samlede indsats sammen.

Regeringen igangsætter 25 initiativer og 6 målrettede strategier for de mest kritiske sektorers arbejde med cyber- og informationssikkerhed, der skal øge den tekniske robusthed i den digitale infrastruktur, øge viden og kompetencer hos borgere, virksomheder og myndigheder og styrke den nationale koordinering og samarbejdet på området. Strategien skal styrke Danmarks cyber- og informationssikkerhed og sikre en systematisk og koordineret indsats i de kommende fire år.

Truslen fra ondsindede cyberangreb kan ikke elimineres, men med en ny strategi for cyber- og informationssikkerhed vil regeringen sikre, at det danske samfund kan fortsætte med at drage nytte af de teknologiske muligheder, og at danskerne fortsat kan være trygge ved den digitale udvikling.

/Regeringen

Digitale muligheder og sårbarheder

Danmark er et af verdens mest digitaliserede lande. Det gælder både i den offentlige sektor, hvor store dele af opgaveløsningen og kommunikationen med borgere er digitaliseret, og i de private virksomheder, som i høj grad udnytter de digitale muligheder til at skabe vækst og nye forretningsmodeller. Og det gælder i den danske befolkning, som er blandt de mest digitaliseringsparate i verden. Den høje grad af digitalisering giver store fordele og mange nye perspektiver for borgere, virksomheder og samfundet som helhed. Blandt andet tiltrækker det investeringer fra udlandet og er med til at sikre, at vores samfund er konkurrencedygtigt.

I de næste mange år vil der ske en fortsat digitalisering af både den offentlige og den private sektor. Udviklingen af nye teknologier vil accelerere, og de digitale muligheder vil fortsat blive flere. Myndigheder vil løbende udnytte digitalisering til at skabe bedre og mere effektiv service til danskerne, og virksomhederne vil bruge mulighederne til at skabe vækst og øget beskæftigelse.

Med den øgede digitalisering af samfundet følger dog også en øget afhængighed af digitale løsninger og dermed en øget sårbarhed overfor hændelser, der medfører nedbrud af it-systemer eller brud på datas fortrolighed, tilgængelighed og integritet. Hændelserne kan fx skyldes angreb eller personers utilsigtede brud på informationssikkerheden. Danske myndigheder og virksomheder har et vigtigt ansvar for at sikre, at sikkerhedstiltagene følger med de udfordringer, som den digitale udvikling også giver.

Med den nationale strategi for cyber- og informationssikkerhed og en række delstrategier for de mest kritiske sektorer lægger regeringen en ambitiøs plan for de kommende års arbejde med at sikre Danmark digitalt. Staten og samfundskritiske sektorer som energi, transport, tele, finans, sundhed og søfart skal i de kommende år øge indsatsen for at sikre det nødvendige cyber- og informationssikkerhedsniveau i hele Danmark.

Arbejdet skal bygge videre på de seneste års nationale indsats, som har medvirket til at løfte niveauet for cyber- og informationssikkerhed, men regeringen vil nu foretage et gearskifte på området. Truslerne udvikler sig med en hast, der kræver, at indsatsen styrkes markant, så den står mål med udfordringerne.

“

Myndigheder og virksomheder har et vigtigt ansvar for at sikre, at sikkerheds-tiltagene følger med udfordringerne

Informationssikkerhed
Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. I arbejdet indgår blandt andet organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger.

Cybersikkerhed
Cybersikkerhed omfatter beskyttelse imod de sikkerhedsbrud, der opstår som følge af angreb mod data eller systemer via en forbindelse til et eksternt net eller system. Arbejdet med cybersikkerhed fokuserer således på sårbarheder ved sammenkoblingen mellem systemer, herunder forbindelser til internettet.

Øget afhængighed og stigende sårbarheder

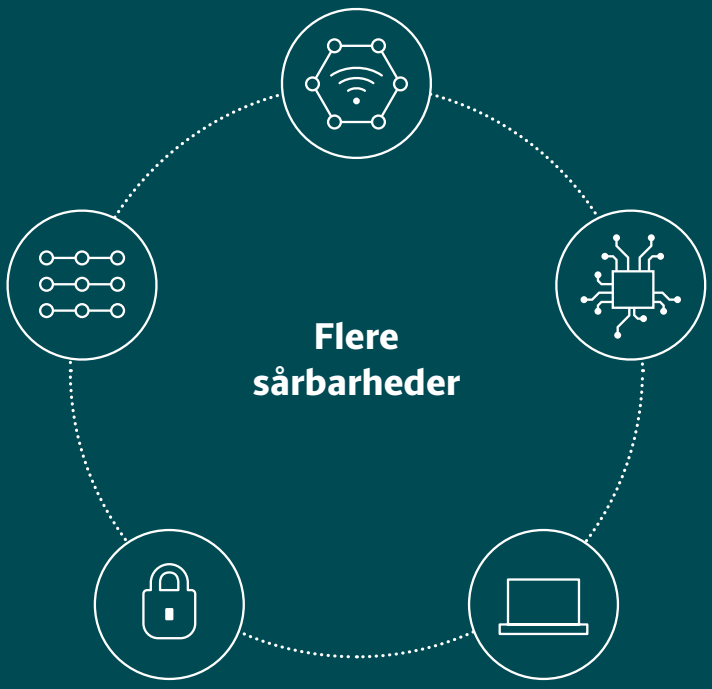
I takt med at det danske samfund i stigende grad forbindes via digitale løsninger, stiger mængden af data og information, der overføres digitalt. Det medfører, at konsekvenserne ved nedbrud eller angreb vokser. Samtidig bliver danske borgere, myndigheder og virksomheder i stigende grad mål for ondsindede aktørers stadigt mere sofistikerede forsøg på at stjæle og udnytte data.

Når systemer og infrastrukturer bliver stadigt mere integrerede, og når flere enheder kobles til internettet, bliver sikkerhedsudfordringerne mere komplekse. Hvad der i første omgang kan virke som en isoleret og relativt lille sikkerhedshændelse kan hurtigt sprede sig på tværs af myndigheder, virksomheder og sektorer.

I mange offentlige myndigheder er der desuden udfordringer med store og komplekse, og i visse tilfælde utidssvarende, it-systemporteføljer, som gør det svært og dyrt at opretholde det nødvendige sikkerhedsniveau. Samtidig understøttes en del af den samfundskritiske it-infrastruktur i en række sektorer som fx finans-, transport- og sundhedssektoren af private virksomheder. Hertil kommer den store mængde af små- og mellemstore virksomheder, som er rygraden i den danske erhvervsstruktur. Hvis de private virksomheder ikke har et tilstrækkeligt sikkerhedsniveau, kan de være kilde til angreb, brud, datalæk og spredning af hændelser til resten af samfundet.

At sikre samfundets robusthed og sikkerhed er dermed blevet en mere kompleks udfordring. Som samfund skal vi ikke alene beskytte os imod forskellige former for angreb, men også imod blandt andet systemnedbrud, leverandørsvigt, tilsigtede og utilsigtede brud på cyber- og informationssikkerheden eller kompromittering af personlige oplysninger.

> **Når systemer og infrastruktur bliver stadig mere integrerede, bliver sikkerhedsudfordringerne mere komplekse**



Utilstrækkelig sikkerhedsadfærd
Manglende sikkerhedsmæssige færdigheder og manglende viden udgør en væsentlig sårbarhed, som kan udnyttes af ondsindede aktører. I myndigheder og virksomheder er ledere og medarbejderes sikkerhedsmæssige adfærd afgørende for at opnå et passende beskyttelsesniveau.

Stor afhængighed af digital infrastruktur
Kritisk digital infrastruktur er en forudsætning for opgavevaretagelsen i den offentlige og private sektor. Manglende tilgængelighed, integritet og fortrolighed i den digitale infrastruktur kan medføre betydelige konsekvenser for samfundet.

Flere enheder er forbundet
Flere og flere enheder forbindes via internettet. Det medfører nye muligheder, men også øget sårbarhed over for angreb som følge af den hurtigere spredning af sikkerhedshændelser.

Stor kompleksitet i it-porteføljen
Mange offentlige og private organisationer er afhængige af komplekse, og ofte gamle, it-systemer. Softwaren i disse systemer er ofte ikke tilstrækkelig vedligeholdt og systemerne har ofte ikke det tilstrækkelige sikkerhedsniveau.

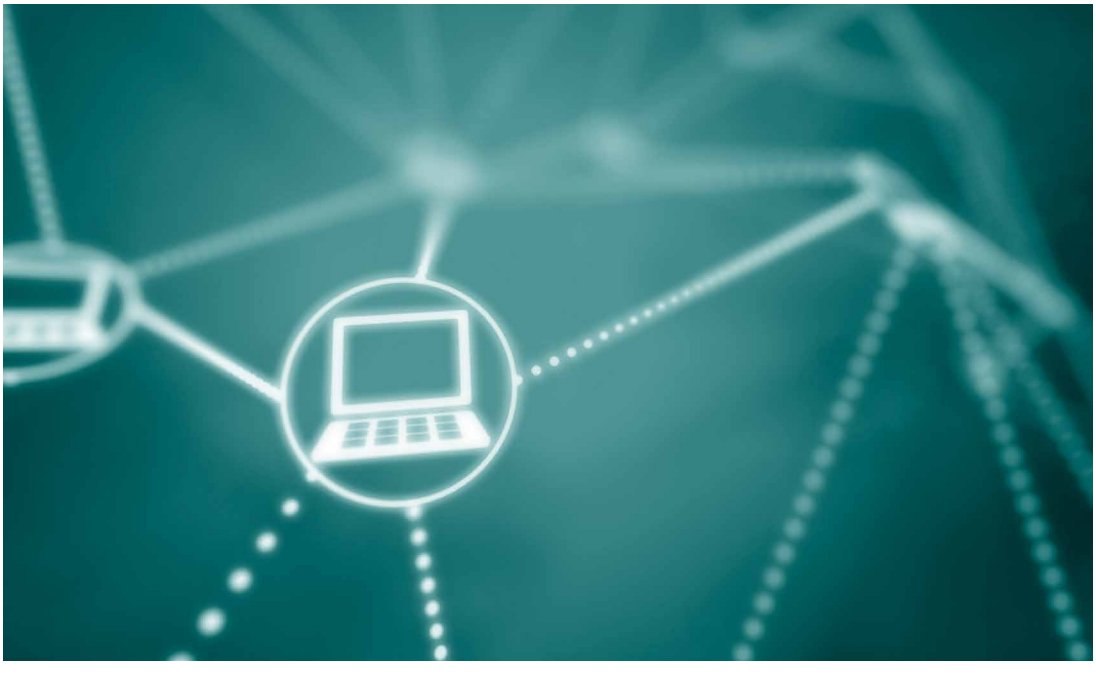
Cyberangreb kan udføres let og billigt
Den lette tilgængelighed til hackerværktøjer på internettet betyder, at de, der ønsker at udføre hackerangreb, kan gøre det relativt let og billigt.

Et trusselsbillede i forandring

Den digitale udvikling har i de senere år givet fx statssponserede grupperinger, fremmede stater, aktivister og kriminelle nye metoder til at udføre cyberrelaterede angreb mod lande, virksomheder og borgere. Det er en global udfordring, som alle åbne og digitaliserede samfund står over for, og som må forventes at blive større i de kommende år.

Cyberangreb kan have mange former og er hændelser, hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester. Det kan eksempelvis være angreb mod myndigheders og virksomheders hjemmesider eller mere avancerede angreb i form af forsøg på at få adgang til fortrolige informationer fra virksomheder og offentlige institutioner – eller ligefrem at forårsage nedbrud eller ødelæggelse.

Truslerne på cyber- og informationssikkerhedsområdet påvirker alle dele af samfundet. Konsekvenserne for ofrene kan variere fra tab af mindre beløb til tab af forretningskritisk information. Angrebene kan få konsekvenser for statens sikkerhed og lede til tab af statens integritet, betydeligt materielt eller økonomisk tab og i yderste instans tab af menneskeliv. For regeringen er det vigtigt, at vi i Danmark løbende tilpasser indsatsen på området til det omskiftelige trusselsbillede.



Truslerne på cyber- og informationssikkerheds-området påvirker alle dele af samfundet

National strategi for cyber- og informationssikkerhed 2015-2016

I Danmarks første nationale strategi for cyber- og informationssikkerhed 2015-2016 var målet at hæve niveauet for det statslige cyber- og informationssikkerhedsarbejde samt at skabe mere viden om cyber- og informationssikkerhed blandt borgere og virksomheder. I strategien indgik blandt andet krav om implementering af den internationale sikkerhedsstandard ISO27001 og krav om et systematisk og professionelt tilsyn med informationssikkerheden i staten.

Strategien indeholdt flere initiativer rettet mod at skabe mere viden blandt borgerne, virksomhederne og myndighederne om cyber- og informationssikkerhed. Center for Cybersikkerhed oprettede en enhed til vurdering af trusler samt et kompetencecenter til rådgivning. Derudover udførte Digitaliseringsstyrelsen kampagneindsatser rettet mod hele befolkningen i strategiperioden. Politiets efterforskningsmæssige kapacitet på området og rådgivning om informationssikkerhed blev styrket. Endelig udviklede Erhvervsstyrelsen et digitalt sikkerhedstjek for særligt små og mellemstore virksomheder, og for at fremme løbende dialog om styrkelse af erhvervslivets rammer for informationssikkerhed blev Virksomhedsrådet for IT-sikkerhed nedsat. Rådet kom i marts 2017 med sine anbefalinger til at styrke it-sikkerheden og fremme ansvarlig datahåndtering hos særligt små og mellemstore virksomheder.

Strategien identificerede også et behov for at styrke dialogen mellem uddannelsesinstitutioner og aftagere af dimittender. Der blev på den baggrund etableret et samarbejde forankret i tre innovationsnetværk med stærke kompetencer inden for cybersikkerhed i forskningen og erhvervslivet. Samarbejdet har blandt andet resulteret i udviklingen af en ny professionsbacheloruddannelse i it-sikkerhed.

En systematisk og vedvarende indsats

Regeringens vision for arbejdet med cyber- og informationssikkerhed i Danmark

- Befolkningen, virksomheder og myndigheder skal kende og kunne håndtere digitale risici, så Danmark fortsat kan udnytte digitaliseringen til at understøtte samfundets udvikling.

Digitaliseringens stigende samfunds- og forretningsmæssige betydning stiller helt nye krav til informationssikkerhed, og de negative konsekvenser ved ikke at have en struktureret tilgang til sikkerhed kan være enorme. Der kræves i dag en systematiseret og koordineret indsats, og derfor sætter regeringen nu styrket fokus på området.

Det er nødvendigt, at Danmark som samfund kan fungere på en sikker og forsvarlig måde. Det kræver, at den digitale infrastruktur er modstandsdygtig over for cybertrusler, og at borgere, virksomheder og myndigheder løbende øger deres digitale kompetencer. Det gælder for sikkerhedsspecialister, som der i de kommende år vil blive endnu større efterspørgsel efter. Og det gælder for den almindelige dansker, hvis viden, om hvordan man færdes sikkert i den digitale verden, løbende skal øges for at understøtte et højt informationssikkerhedsniveau i Danmark.

Et fælles ansvar

Et løft af det nationale niveau for cyber- og informationssikkerhed er et fælles ansvar. Staten har ansvaret for at varetage den nationale sikkerhed. Virksomheder og myndigheder har et ansvar for at varetage sikkerheden i egen organisation. Og alle borgere skal have en forståelse for, hvordan egne handlinger kan påvirke egen og andres digitale sikkerhed.

Regeringen tager med den nationale strategi for cyber- og informationssikkerhed 2018-2021 det næste skridt på vejen mod et mere sikkert digitalt Danmark. Med strategien sætter regeringen ind på tre områder. Der vil ske en teknisk oprustning, samtidig med at borgere, virksomheder og myndigheders viden om cyber- og informationssikkerhed øges, og der sikres styrket samarbejde og koordinering mellem de ansvarlige myndigheder. Samtidig vil delstrategier for cyber- og informationssikkerheden i de mest kritiske sektorer sikre, at den enkelte sektor sætter ind, hvor det er mest nødvendigt.

Private virksomheder ejer og understøtter en stor del af infrastrukturen i sektorer med ansvar for samfundskritiske funktioner. Det er derfor nødvendigt med et stærkt samarbejde både mellem den offentlige og private sektor og mellem det civile samfund, politiet og forsvaret. Strategiens initiativer fokuserer særligt på cyber- og informationssikkerhedsarbejdet i sektorerne energi, transport, tele, finans, sundhed og søfart samt i statslige myndigheder og institutioner.

Regeringen igangsætter 25 konkrete initiativer, som skal medvirke til at styrke cyber- og informationssikkerheden i Danmark. Nogle initiativer bygger videre på indsatser, som allerede er i gang, mens andre initiativer består af helt nye tiltag. Strategien medvirker samtidig til at sammenbinde en række tværgående aktiviteter, som sker i de myndigheder, der har ansvaret for cyber- og informationssikkerheden i Danmark.

En del af en større indsats

Den nationale strategi for cyber- og informationssikkerhed er en del af en større indsats. Regeringen har stort fokus på cybersikkerhed, og med Forsvarsforliget 2018-2023 styrkes Danmarks cyberforsvar markant med en tilførsel af 1,4 mia. kr. over seks år. Det sker blandt andet ved bedre beskyttelse mod avancerede cyberangreb gennem en udbygning af Center for Cybersikkerheds sensornetværk til myndigheder og virksomheder og etablering af et døgnbemandet nationalt cybersituationscenter, hvor der kan dannes et nationalt situationsbillede, som viser aktuelle og potentielle trusler mod Danmarks vigtigste digitale netværk. Center for Cybersikkerhed, som er national it-sikkerhedsmyndighed, får samtidig styrket sin kapacitet til at rådgive og støtte private virksomheder og offentlige myndigheder væsentligt.

EU's direktiv om sikkerhed i net- og informationssystemer i samfundskritiske sektorer – NIS-direktivet

Danske myndigheder er i færd med at implementere et EU-direktiv om sikkerhed i net- og informationssystemer, det såkaldte NIS-direktiv. Direktivet stiller blandt andet krav om, at operatører af væsentlige tjenester, som er af betydning for opretholdelsen af samfundskritiske funktioner og tjenester, træffer foranstaltninger til at håndtere sikkerheden i de net- og informationssystemer, som de anvender ved levering af deres tjenester. Derudover stilles der i direktivet krav om, at medlemsstaterne udarbejder en national strategi for sikkerheden i net- og informationssystemer, hvilket der tages højde for med den nationale strategi for cyber- og informationssikkerhed.

Databeskyttelsesforordningen

En ny databeskyttelsesforordning får virkning den 25. maj 2018. Forordningen suppleres af en ny databeskyttelseslov, der træder i kraft samtidig og understøtter, at beskyttelsen af personoplysninger i Danmark forbedres yderligere.

Som led i en styrkelse af den samlede myndighedsindsats styrkes Forsvarets Efterretningstjenestes arbejde i forhold til påvirkningsoperationer. Blandt andet udbygges Forsvarets Efterretningstjenestes analytiske kapacitet. Endelig fortsætter opbygningen af Forsvarets kapacitet til at udføre militære cyberoperationer.

Forsvarsforligskredsen har reserveret en del af midlerne i forliget til at håndtere fremtidige cyberudfordringer gennem yderligere initiativer, herunder forskning og uddannelse. Det skal sikre, at vi som land kan handle på fremtidige udfordringer.

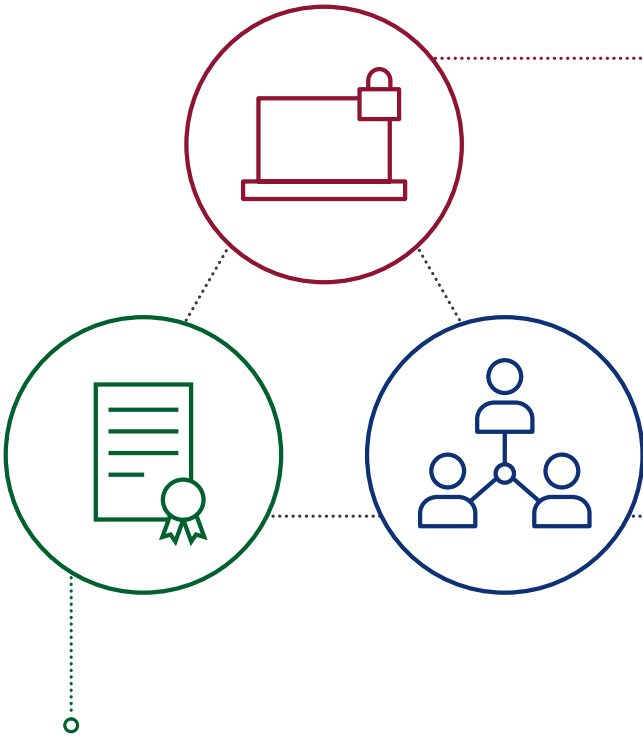
Politiets Efterretningstjeneste planlægger også som national sikkerhedsmyndighed at intensivere samarbejdet med relevante myndigheder og private virksomheder for at bidrage til, at samfundet rustes bedst muligt til at imødegå sikkerhedsmæssige trusler.

Endelig præsenterede regeringen i januar 2018 en strategi for Danmarks digitale vækst, der skal sikre, at Danmark bliver en digital frontløber. Strategien indeholder en række initiativer til at styrke virksomhedernes it-sikkerhed og ansvarlige datahåndtering med henblik på at sikre den digitale tillid til udnyttelsen af de nye teknologiske muligheder.

Sideløbende er det aftalt i den fællesoffentlige digitaliseringsstrategi for 2016-2020, at informationssikkerhedsarbejdet også skal styrkes yderligere i kommuner og regioner. Regeringen vil gå i dialog med kommuner og regioner om yderligere tiltag på området med afsæt i den nationale strategi for cyber- og informationssikkerhed.

Pejlemærker

Regeringen sætter tre klare pejlemærker for udviklingen mod et stærkere og mere sikkert digitalt Danmark i de kommende fire år.



En tryg hverdag for borgere og virksomheder
Staten og samfundskritiske sektorer opruster teknisk i takt med det ændrede trusselsbillede for at være i stand til at beskytte væsentlige samfundsmæssige funktioner mod cyberangreb eller andre større informationssikkerhedshændelser.

Bedre kompetencer
Borgere, virksomheder og myndigheder har adgang til den nødvendige viden og har forudsætningerne for at håndtere de stigende cyber- og informationssikkerhedsudfordringer.

Fælles indsats
Risikobaseret sikkerhedsledelse er en integreret del af styringen i staten og i samfundskritiske sektorer. Der er klarhed over roller og ansvar på cyber- og informationssikkerhedsområdet blandt myndigheder og virksomheder, der leverer samfundskritiske funktioner.

Initiativer

Tryg hverdag

1.1 Etablering af nationalt cybersituationscenter
1.2 Minimumskrav til myndigheders arbejde med cyber- og informationssikkerhed
1.3 Lovgivningsinitiativer på cyberområdet
1.4 Overvågning af statens kritiske it-systemer
1.5 Fælles digital indgang for indberetninger
1.6 Landsdækkende center for behandling af sager vedrørende it-relateret kriminalitet
1.7 Styrket samarbejde om forebyggelse af og håndhævelse over for it-relaterede angreb
1.8 Øget sikring af identitetsbeviser
1.9 Styrket prioritering af national it-infrastruktur
1.10 Sikker kommunikation i staten

Bedre kompetencer

2.1 Digital dømmekraft og kompetencer via uddannelsessystemet
2.2 Informationsportal
2.3 Forskning i ny teknologi
2.4 Erhvervspartnerskab for øget it-sikkerhed i dansk erhvervsliv
2.5 Partnerskab om kompetenceudvikling og opbygning af sikkerhedskultur i staten
2.6 Styrket oplysningsindsats til borgere og virksomheder

Fælles indsats

3.1 Sektorvise delstrategier og decentrale cybersikkerhedsenheder
3.2 Tværgående indsats for at understøtte samfundskritiske sektorers cyber- og informationssikkerhed
3.3 Styr på leverandører af outsourcet it
3.4 Styrket national koordinering
3.5 Styrket internationalt engagement
3.6 Tilstandsmåling af cyber- og informationssikkerhed
3.7 Overblik over beskyttelsesværdig information
3.8 Informationssikkerhedsarkitektur
3.9 National og international indsats for dataetik og persondatabeskyttelse

Tryg hverdag

Initiativer

1.1 Etablering af nationalt cybersituationscenter

1.2 Minimumskrav til myndigheders arbejde med cyber- og informationssikkerhed

1.3 Lovgivningsinitiativer på cyberområdet

1.4 Overvågning af statens kritiske it-systemer

1.5 Fælles digital indgang for indberetninger

1.6 Landsdækkende center for behandling af sager vedrørende it-relateret kriminalitet

1.7 Styrket samarbejde om forebyggelse af og håndhævelse over for it-relaterede angreb

1.8 Øget sikring af identitetsbeviser

1.9 Styrket prioritering af national it-infrastruktur

1.10 Sikker kommunikation i staten

En tryg hverdag for borgere og virksomheder

Pejlemærke: Staten og samfundskritiske sektorer opruster teknisk i takt med det ændrede trusselsbillede for at være i stand til at beskytte væsentlige samfundsmæssige funktioner mod cyberangreb eller andre større informationssikkerhedshændelser.

For at sikre driften af de væsentlige samfundsmæssige funktioner og beskyttelsen af samfundskritiske it-systemer og data vil regeringen blandt andet:

- Skabe bedre overblik over trusler og styrke monitoreringen af samfundskritiske systemer og data
- Hæve myndighedernes cyber- og informationssikkerhedsniveau
- Styrke den nationale rådgivningsindsats

Regeringen vil styrke den nationale robusthed imod cyberangreb. Her udgør viden om trusler, identifikation af sårbarheder og vurdering af risici en stor del af grundlaget. Det er den enkelte virksomhed og myndigheds opgave at sikre egen cyber- og informationssikkerhed og at tilpasse indsatsen på baggrund af risikovurderinger og sårbarhedsanalyser. Hver organisation har ansvaret for, at de nødvendige sikkerhedstiltag er gjort, og at it-systemer og data er tilstrækkeligt beskyttede.

Det kræver overblik og viden om potentielle trusler. Danmarks evne til at afdække og håndtere internetbaserede trusler imod staten og samfundskritiske sektorer skal derfor udvides og styrkes.

Bedre overblik og styrket monitorering

For at beskytte samfundskritiske it-systemer og data er det afgørende, at

de centrale myndigheder har et fyldestgørende overblik over de specifikke systemer og data, der skal beskyttes, samt at der foretages monitorering af vitale systemer og data. Monitoreringen skal muliggøre varsling af myndigheder og virksomheder om potentielle og aktuelle trusler og understøtte, at de beskytter sig og er i stand til at opretholde samfundskritiske funktioner.

For at sikre den løbende monitorering etablerer regeringen et døgnbemandet nationalt cybersituationscenter i Center for Cybersikkerhed. Centeret skal opretholde et nationalt situationsbillede, som viser aktuelle og potentielle trusler mod Danmarks vigtigste digitale netværk, og som vil bidrage til det samlede myndighedsoverblik i det nationale krisestyringssystem.

Der stilles krav om, at myndigheder og visse typer virksomheder indberetter cyberhændelser til de relevante myndigheder. Indberetninger fra myndigheder og virksomheder er en forudsætning for den nødvendige erfaringsopsamling og vidensdeling og for at opretholde et opdateret overblik over antallet af it-sikkerhedshændelser, hændelsestyper og konsekvenser. For at gøre indberetningen lettere vil regeringen etablere én fælles digital løsning til indberetning af it-sikkerhedshændelser. Løsningen skal samtidig kunne levere handlingsorienteret information tilbage til indberetteren om forebyggelse og håndtering af hændelser. En fælles digital løsning vil dels understøtte, at virksomheder og myndigheder indberetter så mange relevante sikkerhedshændelser som muligt, dels medvirke til at skabe et mere nuanceret og detaljeret indblik i de it-sikkerhedshændelser, der rammer danske myndigheder og virksomheder.

Øget myndighedsindsats for cyber- og informationssikkerhed

De statslige myndigheder har siden 2016 være forpligtet til at leve op til kravene i den internationale sikkerhedsstandard ISO27001, der fastsætter bedste praksis for styring af informationssikkerhed. Den seneste opfølgning på de statslige myndighedernes

implementering af ISO27001 viser, at der fortsat udestår et arbejde med at få standarden fuldt ud implementeret. Myndighederne skal blandt andet blive bedre til at foretage risikovurderinger og løbende evaluere indsatsen. Regeringen sætter med strategien øget fokus på at sikre et højt minimumsniveau for it-sikkerhed i alle statslige myndigheder.

Fremover vil alle statslige myndigheder være omfattet af minimumskrav for arbejdet med cyber- og informationssikkerhed. Minimumskravene vil være både tekniske og organisatoriske og skal understøtte en ensartet tilgang til arbejdet og sikre et tilstrækkeligt højt niveau for beskyttelse mod cyber- og informationssikkerhedshændelser. Det betyder, at myndigheder skal blive bedre til at arbejde med risikobaseret informationssikkerhedsledelse gennem ISO27001, udarbejde handlingsplaner for håndtering og udvikling af it-porteføljen, herunder håndtering af legacy-udfordringer og informationssikkerhed, tage aktivt og dokumenteret stilling til vejledningsprodukter på området og implementere kendt og velafprøvet teknologi til beskyttelse mod angreb.

For at sikre fuld implementering af ISO27001 i statslige myndigheder vil regeringen fremadrettet følge op på myndighedernes implementering hvert halve år. Regeringen vil stille krav om, at de myndigheder, der endnu ikke er i mål, skal forelægge en handleplan for regeringen, som beskriver hvilke indsatser, der vil blive gennemført med henblik på at sikre fuld implementering af standarden.

Styrket national rådgivningsindsats

Center for Cybersikkerhed er national it-sikkerhedsmyndighed og står for en forebyggende, national rådgivnings- og oplysningsvirksomhed om cybersikkerhed i forhold til både den offentlige og den private sektor samt en målrettet indsats i forhold til håndtering af konkrete hændelser.

Med Forsvarsforliget 2018-2023 styrkes centerets forebyggende indsats væsentligt gennem styrket rådgivning og vejledning til især samfundskritiske sektorer.

Samtidig styrkes centerets kapacitet til at opdage konkrete hændelser. Sammen med centerets rådgivning skal det bidrage til de ansvarlige myndigheder og virksomheders arbejde med at genoprette sikkerheden efter cyberangreb inden for samfundsvigtige sektorer.

Risikobaseret tilgang

Myndighedernes og virksomhedernes arbejde med informationssikkerhed skal ske med udgangspunkt i en risikovurdering. Denne omfatter en vurdering af, hvilke forretningsmæssige og økonomiske risici der er for opretholdelsen af de forretningsmæssige mål ved mulige sikkerhedshændelser, herunder cyberangreb, og hvad der er passende sikkerhedsforanstaltninger med henblik på at nedbringe risikoen til et acceptabelt niveau.

Vurderingen forudsætter et overblik over organisationens systemer, herunder deres tekniske udformning og sårbarheder. Med udgangspunkt i den prioritering, som er fastlagt i risikovurderingen, iværksættes passende tiltag for at imødegå de identificerede sårbarheder.

Regeringens initiativer – Tryg hverdag

Initiativ 1.1: Etablering af nationalt cybersituationscenter

Der oprettes et døgnbemandet nationalt cybersituationscenter ved Center for Cybersikkerhed for at etablere et nationalt situationsbillede af den aktuelle sikkerhedstilstand for samfundskritiske digitale netværk. Situationscentret skal foretage teknisk monitorering af netværk, scanne efterretningskilder, medier og fora for oplysninger om nye trusler og igangværende potentielt alvorlige cyberangreb og samtidig fungere som nationalt kontaktpunkt i forhold til grænseoverskridende cybersikkerhedshændelser.

Initiativ 1.2: Minimumskrav til myndigheders arbejde med cyber- og informationssikkerhed

Der skal sikres et tilstrækkeligt minimumsniveau for håndtering af cyber- og informationssikkerhed i statslige myndigheder. Alle statslige myndigheder skal følge principperne i informationssikkerhedsstandarden ISO27001 og foretage en vurdering af behovet for certificering. De myndigheder, der ikke er i mål med implementeringen, skal forelægge en handleplan for regeringen med henblik på at sikre fuld implementering af standarden. Myndighederne skal desuden tage aktivt og dokumenteret stilling til anvendelse af vejledninger om cyber- og informationssikkerhed, vurdere behovet for at implementere kendte og velafprøvede teknologier til beskyttelse mod ondsindede cyber- og informationssikkerhedshændelser samt følge kravene i Strategi for it-styring i staten.

Initiativ 1.3: Lovgivnings-initiativer på cyberområdet

Den hastige udvikling i trusselsbilledet medfører behov for at tilpasse lovgivningen til både det aktuelle trusselsbillede og den teknologiske udvikling, så Center for Cybersikkerhed får bedre muligheder for at imødegå cyberangreb mod den kritiske infrastruktur. Forsvarsministeriet vil derfor fremsætte et forslag til ændret lovgivning på cyberområdet, som vil medføre en styrkelse af Center for Cybersikkerheds muligheder for at opdage og stoppe cyberangreb samt styrke centerets analytiske arbejde.

Initiativ 1.4: Overvågning af statens kritiske it-systemer

Som følge af udviklingen i trusselsbilledet er der behov for at udbygge den proaktive overvågningsindsats for sikringen af statens kritiske it-systemer. Der etableres derfor et døgnbemandet overvågningscenter i Statens It. Initiativet vil give alle Statens Its kunder muligheden for døgnovervågning af systemer, der driftes i Statens It. Initiativet vil blive indfaset over tid med et fuldt funktionsdygtigt overvågningscenter i 2020. Myndigheder, hvis systemer ikke driftes i Statens It, skal sikre sig, at der er 24/7 driftsovervågning, hvis det ud fra en risikovurdering findes nødvendigt.

Initiativ 1.5: Fælles digital indgang til indberetninger

Det skal være nemt og enkelt for virksomheder og myndigheder at indberette sikkerhedshændelser. Derfor etableres der én fælles digital løsning for indberetning af sikkerhedshændelser. Løsningen skal understøtte, at virksomhederne kun skal indberette hændelser én gang, ét sted og skal samtidig kunne levere handlingsorienteret information tilbage til indberetteren om forebyggelse og håndtering af hændelser. Løsningen placeres på Virk.dk, som allerede i dag er den digitale indgang for virksomheder og myndigheder i forhold til indberetninger til det offentlige.

Initiativ 1.6: Landsdækkende center for behandling af sager vedrørende it-relateret kriminalitet

For at sikre en ensartet og styrket indsats imod it-relateret kriminalitet, etableres der i dansk politi et landsdækkende center for modtagelse og indledende håndtering af anmeldelser om it-relateret kriminalitet. Centeret vil bidrage til, at politiet i højere grad kan arbejde databaseret i bekæmpelsen og forebyggelsen af kriminalitet.

Initiativ 1.7: Styrket samarbejde om forebyggelse af og håndhævelse over for it-relateret kriminalitet

It-relaterede angreb kan begås med en stor afstand mellem gerningsperson og offer og via tekniske løsninger, der kan udfordre sædvanlige og kendte metoder til bekæmpelse heraf. Det er derfor vigtigt, at de relevante myndigheder har de redskaber og kapaciteter, der skal til for effektivt at forhindre angreb i at opstå eller udvikle sig. Det eksisterende samarbejde mellem myndigheder med et tværgående ansvar på området skal løbende sikre det bedste grundlag for at kunne bekæmpe it-relaterede angreb. Med henblik på at sikre dette etableres en arbejdsgruppe med deltagelse af Forsvarsministeriet og Justitsministeriet.

Initiativ 1.8: Øget sikring af identitetsbeviser

Som samfund skal vi kunne have tillid til de identiteter og identitetsbeviser, som oprettes og udstedes af myndighederne. Det gælder både for fysiske og digitale identitetsbeviser som fx pas, kørekort og NemID. Der igangsættes derfor en indsats for at sikre sammenhæng mellem registrering af en fysisk identitet og udstedelse af en digital identitet samt sikre sammenhæng på tværs af forskellige systemer i den offentlige sektor.

Initiativ 1.9: Styrket prioritering af national it-infrastruktur

Der skal udarbejdes en fyldestgørende oversigt over myndigheder og virksomheder med digital infrastruktur, der er væsentlige for samfundskritiske funktioner. Der gennemføres en beskrivelse af, hvilke centrale virksomheder og myndigheder og eventuelt tjenester, der har en særlig betydning for arbejdet med cyber- og informationssikkerheden i Danmark. Beskrivelsen vil sammenholdt med en trusselvurdering danne grundlag for en styrket prioritering af Center for Cybersikkerheds monitorering og sektoransvarlige myndigheder og virksomheders imødegåelse af cyberangreb, samt for det løbende arbejde med cyber- og informationssikkerhed i bred forstand.

Initiativ 1.10: Sikker kommunikation i staten

Der er behov for bredere adgang til sikkert at kommunikere mellem myndigheder. Der etableres derfor bedre mulighed for, at statslige myndigheder kan anvende netværk med et højt sikkerhedsniveau til at kommunikere med hinanden, ligesom en løsning til sikker mobiltelefonkommunikation udbredes.

2

Bedre kompetencer

Initiativer

2.1 Digital dømmekraft og kompetencer via uddannelsessystemet

2.2 Informationsportal

2.3 Forskning i ny teknologi

2.4 Erhvervspartnerskab for øget it-sikkerhed i dansk erhvervsliv

2.5 Partnerskab om kompetenceudvikling og opbygning af sikkerhedskultur i staten

2.6 Styrket oplysningsindsats til borgere og virksomheder

Bedre kompetencer

Pejlemærke: Borgere, virksomheder og myndigheder har adgang til den nødvendige viden og har forudsætningerne for at håndtere de stigende cyber- og informationssikkerhedsudfordringer.

For at understøtte bedre kompetencer blandt borgere, virksomheder og myndigheder vil regeringen blandt andet:

- Hæve den digitale dømmekraft og de digitale kompetencer hos børn og unge
- Øge viden om cyber- og informationssikkerhed hos borgere, virksomheder og myndigheder
- Styrke arbejdet med løbende at opbygge mere specialiseret viden og ekspertise på området.
- Styrke indsatsen for bedre cyber- og informationssikkerhed i erhvervslivet

Den øgede digitalisering og konstante forandring i trusselsbilledet stiller større og større krav til den enkelte borgers, virksomheds og organisations viden om digital sikkerhed og kompetencer for at imødegå cyber- og informationssikkerhedstrusler.

Den hastige udvikling af nye teknologier, sammenholdt med de kriminelles evne til at udnytte dem, vil konstant skabe nye udfordringer. Der er derfor behov for, at danskernes viden om cyber- og informationssikkerhed øges, og at borgere og virksomheders digitale adfærd bliver mere sikker.

Digital dømmekraft og kompetencer via uddannelsessystemet

Mange unge ved ikke nok om, hvordan de beskytter sig selv og andre på internettet, eller hvilke aktører de skal være opmærksomme på. Uddannelsessystemet spiller her en vigtig rolle i at sikre, at alle børn og unge klædes på

til at begå sig trygt, forsvarligt og etisk korrekt, når de anvender it og bevæger sig på sociale medier.

Regeringen vil derfor sætte fokus på digitale færdigheder i et sikkerhedsperspektiv i undervisningen allerede fra folkeskolen og hele vejen op i uddannelsessystemet. Børn og unge skal have de bedste muligheder for at gribe de digitale muligheder og til at agere kritisk som borgere i et digitaliseret samfund. Børn og unge skal have evnerne til at tænke kritisk i forhold til indhold på internettet, så de er opmærksomme på truslen fra falske nyheder, radikalisering, cybermobning, svindel mv. De skal kunne færdes sikkert på internettet og udnytte de digitale muligheder på en tryg og sikker måde, ligesom de skal være bevidste om, hvilke regler og konsekvenser, der følger af at begå sig online. Børn og unge skal gøres digitalt kompetente og opbygge en stærk digital dømmekraft med forståelse af de etiske dilemmaer, der ligger ud over den tekniske forståelse af digitaliseringen.

> **Børn og unge skal have evnerne til at udnytte de digitale muligheder på en tryg og sikker måde**

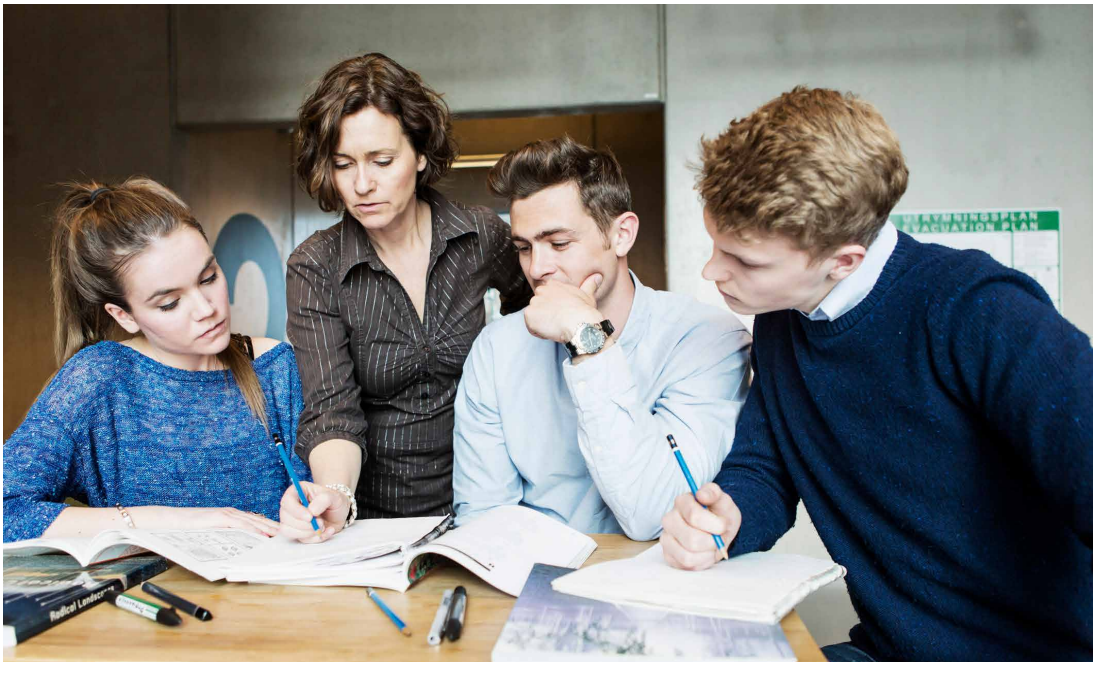
Øget viden om cyber- og informationssikkerhed

Der skal hos alle borgere, myndigheder og virksomheder være kendskab til og kontinuerlig forbedring af bevidstheden om cybertrusler, og hvordan de imødegås med sikker adfærd – og også hvilke risici, man udsætter sig selv og andre for.

Regeringen etablerer derfor en informationsplatform til vidensformidling rettet mod borgere, virksomheder og myndigheder. Borgere, virksomheder og myndigheder skal kunne finde relevant og konkret anvendelig viden om og værktøjer til, hvordan de bedst beskytter sig. Informationsindsatser skal medvirke til at skabe større opmærksomhed om trusler, og informationsportalen skal understøtte et højere vidensniveau, der gør befolkningen i stand til at tage de fornødne forholdsregler.

I takt med den teknologiske udvikling stiger udfordringen med at sikre cyber- og informationssikkerheden i de statslige myndigheder, og de rette kompetencer vil blive stadig mere efterspurgte – både blandt specialister og generalister. Samtidig oplever den private sektor en øget efterspørgsel efter kvalificeret arbejdskraft. Regeringen vil derfor invitere alle relevante parter til at medvirke i et partnerskab om kompetenceopbygning på området.

For at øge kompetencerne på det statslige område igangsætter regeringen derudover en række initiativer, der er målrettet ledere, medarbejdere og specialister i staten, så de fortsat kan udvikle og digitalisere den statslige sektor med det nødvendige sikkerhedsniveau. En del af kurserne på det



statslige digitaliseringsakademi, som regeringen præsenterede i efteråret 2017 som led i "Strategi for it-styring i staten", vil derfor omhandle sikker digital adfærd samt have et grundlæggende fokus på cyber- og informationssikkerhed.

Viden om ny teknologi

Ud over behovet for øget viden er der behov for flere sikkerhedsspecialister til at understøtte en sikker digital omstilling af virksomheder og myndigheder. Disse særlige færdigheder er vitale i den digitale tidsalder og helt afgørende for Danmarks evne til at opretholde cyber- og informationssikkerheden.

Regeringen vil med mere fokuseret forskning i ny teknologis betydning for digitale sårbarheder generere mere viden om de bedst mulige foranstaltninger, modeller og værktøjer for cyber- og informationssikkerhed. Det skal ske ved at sætte strategiske forskningsmidler af til at forske i nye teknologiske muligheder.

Forskning på området skal også bidrage til mere kvalificeret undervisning i cybersikkerhed på uddannelsesinstitutionerne og dermed understøtte, at fremtidens arbejdsstyrke får de nødvendige færdigheder og den ekspertise, der efterspørges af de danske virksomheder.

Styrket indsats for bedre cyber- og informationssikkerhed i erhvervslivet

Regeringen vil understøtte en generel styrkelse af cyber- og informationssikkerheden i dansk erhvervsliv. Danske virksomheder har som resten af det danske samfund været gode til at tage digitaliseringen til sig. Arbejdsgange er

blevet automatiseret, papirarkiver og regnskabsbøger er digitaliseret og lagt ind i it-systemer og salg og markedsføring foregår i stigende omfang via internettet. Det gavner virksomhedernes vækst og konkurrenceevne, men afhængigheden af digitale systemer øger også virksomhedernes sårbarhed overfor cyberangreb.

Danske virksomheder udsættes i stigende grad for cyberangreb. Et cyberangreb kan have voldsomme konsekvenser for den enkelte virksomhed, men samtidig er de mange små- og mellemstore virksomheder en potentiel kilde til angreb, brud, datalæk og spredning af hændelser.

Regeringen sætter nu fokus på at styrke cyber- og informationssikkerheden i dansk erhvervsliv. Opgaven skal løftes i samarbejde med erhvervslivets interessenter, og derfor etableres et partnerskab for øget it-sikkerhed og ansvarlig datahåndtering i dansk erhvervsliv.

Erhvervspartnerskabet skal danne rammen om en fælles indsats for at fremme it-sikkerhed og ansvarlig datahåndtering og skabe grobund for udbredelse af fælles løsninger på tværgående problemer. Gennem partnerskabet udvikles forebyggende sikkerhedstiltag, der iværksættes en indsats for at fremme virksomhedernes anvendelse af internationale sikkerhedsstandarder, og endelig vil partnerskabet have fokus på, hvordan der kan iværksættes en indsats for at styrke virksomhedernes primære rådgiveres indsigt i it-sikkerhed, så de kan fungere som brobyggere, der fremmer it-sikkerhed i danske små og mellemstore virksomheder.

Regeringen har desuden med Strategi for Danmarks digitale vækst besluttet at videreføre Virksomhedsrådet for IT-sikkerhed, som løbende skal komme med anbefalinger til regeringen og dansk erhvervsliv om styrkelsen af rammerne for virksomhedernes it-sikkerhed og ansvarlige datahåndtering. Rådet får en rolle som advisory board for partnerskabet og kan komme med anbefalinger og input om konkrete virksomhedsrettede løsninger.

Teknologipagt

Danske virksomheder oplever i dag stor mangel på ansatte med digitale og tekniske kompetencer. I takt med at avanceret teknologi og digitale løsninger udbredes i fremtiden, vokser virksomhedernes efterspørgsel efter fx ingeniører, dataloger, biostatistikere, elektrikere og andre personer med digitale og tekniske færdigheder. Derfor har regeringen igangsat en Teknologipagt, der skal få flere unge til at interessere sig, uddanne sig og arbejde indenfor det digitale og tekniske område.

Regeringen har med Teknologipagten sat et mål om, at 20 pct. flere skal gennemføre en faglært eller videregående uddannelse over de næste 10 år indenfor de såkaldte STEM-områder (teknologi, it, naturvidenskab og matematik).

Kilde: Strategi for Danmarks digitale vækst

Regeringens initiativer – Bedre kompetencer

Initiativ 2.1: Digital dømmekraft og kompetencer via uddannelsessystemet

Der igangsættes en samlet indsats i hele uddannelseskæden med fokus på at øge opmærksomheden om sikkerhedsudfordringer for børn, unge og undervisere. Der udarbejdes bl.a. efter- og videreuddannelsesforløb, undervisningsmateriale samt kampagner om cyber- og informationssikkerhed rettet mod både undervisere, elever og studerende.

Initiativ 2.2: Informationsportal

Der etableres en informationsportal, der bl.a. skal indeholde lettilgængelig og handlingsanvisende information og konkrete værktøjer til borgere, virksomheder og myndigheder vedr. informationssikkerhed og databeskyttelse samt information om, hvordan gældende lovgivning efterleves. Indholdet på portalen skal være dynamisk, aktuelt og løbende opdateret med den nyeste viden.

Initiativ 2.3: Forskning i ny teknologi

Regeringen vil prioritere flere midler til teknologisk forskning, herunder midler til FORSK2025-temaet "Nye teknologiske muligheder" til udmøntning i Danmarks Innovationsfond. Forskningsindsatsen skal bl.a. fokusere på at skabe viden omkring nye modeller og værktøjer til at vurdere trusler, viden til at styrke infrastrukturen imod angreb samt viden, der kan medvirke til at forbedre myndigheder og virksomheders evner til at identificere angribere.

Initiativ 2.4: Erhvervspartnerskab for øget it-sikkerhed i dansk erhvervsliv

Regeringen ønsker at styrke it-sikkerhed og ansvarlig datahåndtering i dansk erhvervsliv og bidrage til, at det bliver en dansk styrkeposition. For at sikre dette er det nødvendigt, at der løftes i flok på tværs af den offentlige og private sektor, ligesom der er behov for en tæt dialog og vidensudveksling mellem de aktører, der på forskellig vis kan understøtte virksomhedernes arbejde med it-sikkerhed og ansvarlig datahåndtering. Regeringen vil derfor tage initiativ til at etablere et offentlig-privat samarbejde i form af et erhvervspartnerskab for øget it-sikkerhed og ansvarlig datahåndtering. Samtidig videreføres Virksomhedsrådet for IT-sikkerhed og får en rolle som advisory board for Erhvervspartnerskabet.

Initiativ 2.5: Partnerskab om kompetenceudvikling og opbygning af sikkerhedskultur i staten

Kompetencer relateret til cyber- og informationssikkerhed vil blive stadig mere efterspurgt – både blandt specialister og generalister. Regeringen inviterer derfor alle relevante parter til at medvirke i et partnerskab om kompetenceopbygning på området. Derudover iværksættes en række tiltag for kompetenceudvikling af statsligt ansatte. De ansatte skal have forudsætningerne for at fortsætte udviklingen og digitaliseringen af den statslige sektor med det nødvendige sikkerhedsniveau.

Initiativ 2.6: Styrket oplysningsindsats til borgere og virksomheder

Der er behov for at styrke oplysningsindsatsen rettet mod borgere og virksomheder for at styrke sikker adfærd på nettet og skabe løbende opmærksomhed på området. Der skal gennemføres landsdækkende oplysningsindsatser suppleret af målrettede indsatser mod grupper af borgere og virksomheder, der er særligt udfordrede på den digitale kommunikation, og lokale indsatser rettet mod fx virksomheder eller særlige medarbejdergrupper i den offentlige sektor. Private og offentlige parter inviteres til at deltage som bidragsydere og partnere til indsatserne.

3

Fælles indsats

Initiativer

3.1 Sektorvise delstrategier og decentrale cybersikkerhedsenheder

3.2 Tværgående indsats for at understøtte samfundskritiske sektorers cyber- og informationssikkerhed

3.3 Styr på leverandører af outsourcet it

3.4 Styrket national koordinering

3.5 Styrket internationalt engagement

3.6 Tilstandsmåling af cyber- og informationssikkerhed

3.7 Overblik over beskyttelsesværdig information

3.8 Informationssikkerhedsarkitektur

3.9 National og international indsats for dataetik og persondatabeskyttelse

Fælles indsats

Pejlemærke: Risikobaseret sikkerhedsledelse er en integreret del af styringen i staten og i samfundskritiske sektorer. Der er klarhed over roller og ansvar på cyber- og informationssikkerhedsområdet blandt myndigheder og virksomheder, der leverer samfundskritiske funktioner.

For at sikre en fælles indsats på cyber- og informationssikkerhedsområdet vil regeringen blandt andet:

- Iværksætte en indsats for at understøtte samfundskritiske sektorers arbejde med cyber- og informationssikkerhed
- Stille større krav til myndigheders styring af leverandører af samfundskritiske it-systemer
- Styrke den strategiske koordination på nationalt niveau
- Styrke Danmarks internationale engagement på området

Opgaverne på cyber- og informationssikkerhedsområdet varetages af en række forskellige myndigheder med forskellige roller. Den fortsatte digitalisering og de stadig flere gensidige digitale afhængigheder i samfundet medfører behov for øget koordination mellem myndigheder på området. Det kræver en højere grad af central, strategisk forankring af indsatser og tiltag på nationalt niveau.

Karakteren af de sikkerhedsmæssige udfordringer betyder, at cyber- og informationssikkerhed i dag skal være et vigtigt fokusområde for alle ledere, såvel offentlige som private. Samtidig er cyber- og informationssikkerheden i Danmark afhængig ikke blot af statens indsats på området, men i lige så høj grad af indsatsen i de samfundskritiske sektorer. Der er således behov for at understøtte arbejdet med cyber- og

informationssikkerhed både centralt i staten, i sektorerne og i forhold til borgere og det brede erhvervsliv gennem øget erfaringsudveksling og koordinering. Det vil både bidrage til at løfte Danmarks sikkerhed og medvirke til at gøre fokus på cyber- og informationssikkerhed til en strategisk mulighed for øget vækst og velstand og ikke blot en operationel udfordring.

Styrket indsats i samfundskritiske sektorer

For at opretholde cyber- og informationssikkerheden i hele Danmark er det afgørende, at der i samfundskritiske sektorer er det nødvendige fokus på området. Derfor igangsætter regeringen en række initiativer, der skal løfte de samfundskritiske sektorers arbejde med cyber- og informationssikkerhed.

Forskellige modenhedsniveauer og behov i de enkelte sektorer betyder, at indsatsen skal differentieres i de forskellige sektorer. Der etableres dedikerede cyber- og informationssikkerhedsenheder, som skal bidrage til at gennemføre sektorvise trusselsvurderinger, styrke monitoreringen, sikkerheds- og kompetenceopbygge og rådgive og vejlede myndigheder og virksomheder i sektorerne.

Sektorspecifikke strategier

Sektorer, der har særlig betydning for cyber- og informationssikkerheden i Danmark, skal sikre, at der ligger en klar plan for arbejdet med cyber- og informationssikkerhed i sektorerne. Sektorerne skal derfor udarbejde sektorspecifikke strategier, der tager udgangspunkt i de særlige forhold, der gør sig gældende i sektorerne. Sektorerne skal under udarbejdelsen af delstrategierne inddrage relevante interessenter i arbejdet.

> “Cyber- og informationssikkerheden i Danmark er i høj grad afhængig af indsatsen i samfundskritiske sektorer

Energi
En sikker energiforsyning er en forudsætning for et velfungerende samfund, og manglende sikkerhed i sektoren er dermed en sårbarhed for hele samfundet. Energisektorernes sårbarhed overfor cybertrusler udvikler sig hastigt i takt med digitalisering af alt fra vindmøller til husholdningsapparater. Leverandører af digitalt udstyr, software eller overvågning vil i fremtiden have en øget betydning for leverancen af energi. Samtidig er der en øget afhængighed af digital styring af anlæg til energiudvekslingen med nabolandende og balanceringen af fluktuerende energiproduktion fra sol- og vindenergi. Derfor er der fastsat regler for el- og naturgassektorernes beredskab og herunder specifikt it-beredskabet, således at nye trusler, sårbarheder og risici erkendes og håndteres i tide. Energisektorernes delstrategi skal bygge videre på det arbejde inden for de eksisterende rammer.

Energi- Forsynings- og Klimaministeriet har ansvaret for senest med udgangen af 2018 at have udarbejdet en delstrategi for cyber- og informationssikkerheden i energisektorerne.

“

Regeringen igangsætter initiativer, der skal løfte samfundskritiske sektorers arbejde med cyber- og informationssikkerhed

Sundhed
Sundhedssektoren er kendetegnet ved, at der ved behandling og pleje af patienter registreres et stort antal personhenførbare oplysninger i forbindelse med journalføring, dokumentationskrav, indberetning til registre, ligesom der anvendes digitalt apparatur og medicinsk udstyr mv. Det bidrager til at gøre sektoren til et muligt mål for cyberkriminalitet, hvor udefrakommende personer hacker sig til adgang til disse oplysninger og systemer. Det udbredte samarbejde om patientbehandlingen i sundhedssektoren med dertilhørende deling af patientoplysninger parterne imellem indebærer desuden en risiko for, at potentielle cyberkriminelle vil gå efter “det svageste led”, hvis ikke alle aktører i tilstrækkelig grad lever op til nødvendige og ensartede krav til sikkerhed. Delstrategien skal på den baggrund styrke og ensrette arbejdet med cyber- og informationssikkerhed på tværs af sundhedssektoren med henblik på at forudsige, forebygge, opdage og håndtere cyberangreb samt videreføre arbejdet i strategi for digital sundhed 2018-2022, hvor blandt andet cyberpolitisk forum sætter cybersikkerhed på dagsordenen i hele sundhedssektoren.

Sundheds- og Ældreministeriet har ansvaret for senest med udgangen af 2018 at have udarbejdet en delstrategi for cyber- og informationssikkerheden i sundhedssektoren.

Transport
Kritisk infrastruktur i transportsektoren understøttes i stigende grad af it-systemer, der tillader centraliseret monitorering og fjernstyret eller automatiseret kontrol. I takt med digitaliseringen stiger truslen for angreb rettet

mod funktioner og systemer, som er kritiske for at sikre en transportsektor med høj mobilitet og sikker trafikafvikling. Udarbejdelsen af en delstrategi for cyber- og informationssikkerheden vil omfatte hele ressortområdet. Det er dog primært luftfartsområdet, og i nogen grad jernbaneområdet, der er afhængige af netværks- og informationssystemer og dermed kan være sårbare over for trusler mod cyber- og informationssikkerheden. Delstrategien vil skabe overblik over de udfordringer, som transportsektoren står overfor som følge af stigende anvendelse af elektroniske styringssystemer og automatiseret dataudveksling. Den vil dermed udgøre grundlaget for den overordnede prioritering af arbejdet med cyber- og informationssikkerhed i transportsektoren med fokus dels på at sikre opretholdelse af samfundskritiske transportfunktioner og dels på passagerernes sikkerhed.

Transport-, Bygnings- og Boligministeriet har ansvaret for senest med udgangen af 2018 at have udarbejdet en delstrategi for cyber- og informationssikkerheden i transportsektoren.

Tele

Telesektoren er kendetegnet ved, at det samlede telenet er en af de mest kritiske dele af samfundets it-infrastruktur. På teleområdet har regeringen gennem etablering af lov om net- og informationssikkerhed derfor haft fokus på at sikre, at teleudbyderne opretholder en høj grad af informationssikkerhed. Det indebærer, at teleudbyderne skal sikre tilgængelighed, integritet og fortrolighed i deres telenet, ligesom teleudbyderne skal have et beredskab, der understøtter, at samfundets funktioner i videst muligt omfang kan videreføres i tilfælde af, at telenettet påvirkes af ulykker, katastrofer og cyberangreb.

Forsvarsministeriet har ansvaret for senest med udgangen af 2018 at have udarbejdet en delstrategi for cyber- og informationssikkerheden i telesektoren.

Finans
I den finansielle sektor har man etableret et sektorforum i form af Finansielt Sektor forum for Operationel Robusthed (FSOR), som blandt andet skal være med til at sikre en fælles, koordineret indsats i forhold til cyber- og informationssikkerhed. Endvidere implementeres NIS-direktivet i den finansielle lovgivning inden maj 2018. Delstrategien vil supplere implementeringen af NIS-direktivet og bygge videre på det allerede etablerede sektorforum, FSOR, med konkrete initiativer, som med udgangspunkt i sektorens sårbarheder og aktuelle modenhed bidrager til øget robusthed over for cyberangreb og dermed øget cybersikkerhed i finanssektoren.

Erhvervsministeriet har ansvaret for senest med udgangen af 2018 at have udarbejdet en delstrategi for cyber- og informationssikkerheden i finanssektoren.

Søfart
Søfartssektorens sektoransvar omfatter sikkerheden for sejlads i danske farvande samt sikkerheden for danskflagede skibe og deres besætning. Cybersikkerhed for skibe omfatter tjenester som trafikovervågning, advarsler og information til skibsfarten (AIS, NAVTEX), skibssystemer og software til skibets drift, herunder til fremdrivning og navigation. Delstrategien vil supplere implementeringen af NIS-direktivet med konkrete initiativer, som med udgangspunkt i sektorens sårbarheder og aktuelle modenhed bidrager til øget robusthed over for cyberangreb og dermed øget cybersikkerhed i søfartssektoren.

Erhvervsministeriet har ansvaret for med udgangen af 2018 at have udarbejdet en delstrategi for cyber- og informationssikkerheden i søfartssektoren.

Drikkevandsforsyning
Der vil ikke blive udarbejdet en særskilt delstrategi for drikkevandsforsyningssektoren, da leverancen af drikkevand ikke er afhængig af net- og informationssystemer, idet alle forsyningsselskaber har mulighed for manuel drift. Kommunerne har imidlertid en forpligtelse til at have en beredskabsplan, der sikrer leverancen af drikkevand.

Det kan ikke udelukkes, at der med tiden vil ske ændringer i forsyningernes drift hen imod en afhængighed af it-styring af drikkevandsleverancen. Miljø- og Fødevareministeriet vil

Cyberpakke

EU-Kommissionen har fremlagt en omfattende cyberpakke med det overordnede formål at skabe modstandsdygtighed, afskrækkelse og forsvare Europa mod cybertrusler – og samtidig øge de europæiske borgeres tillid til digitale løsninger. Cyberpakken bygger videre på de fremskridt, der blev gjort med EU's cyberstrategi fra 2013, hvor særligt net- og informationssikkerhedsdirektivet (NIS-direktivet) stod centralt. EU-Kommissionens cyberpakke indeholder en lang række tiltag, herunder et forordningsforslag til styrkelse af EU's Cyberagenturs (ENISA) mandat samt en fælleseuropæisk ramme for cybersikkerhedscertificering.

> **Regeringen vil skabe bedre sammenhæng mellem de operationelle tiltag og den overordnede strategiske tilgang til cyber- og informationssikkerhed**

løbende vurdere, om der vil skulle udarbejdes en delstrategi i sektoren.

Domænenavnssystemer og digitale tjenester

NIS-direktivet stiller krav om, at udbydere af såkaldte domænenavnssystemer og administratorer af topdomænenavne samt udbydere af visse digitale tjenester, herunder blandt andet cloud computing-tjenester, skal styre risici i forhold til sikkerheden i deres tjenester og indberette væsentlige sikkerhedshændelser. Disse krav bliver implementeret med Erhvervsministeriets kommende lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester.

Styr på leverandører af samfundskritisk it

En stor del af danske myndigheders samfundskritiske it-systemer drives af private leverandører. Det stiller store krav til myndighederne om at sikre, at deres leverandører opretholder et passende sikkerhedsniveau, at data og informationer behandles i overensstemmelse med lovgivningen, og at borgernes rettigheder i forhold til deres personoplysninger respekteres.

Regeringen indfører derfor skærpede krav til alle offentlige myndigheder om brug af tilstrækkelige sikkerheds- og styringsbestemmelser i fremtidige kontrakter for samfundskritiske it-systemer samt til myndighedernes styring af private leverandører. Endelig vil regeringen undersøge muligheden for at give staten hjemmel til om nødvendigt og i helt særlige tilfælde at overtage samfundskritiske it-systemer, der drives for en myndighed.

Mere samarbejde og øget national koordinering

Sektoransvarsprincippet betyder, at den myndighed, der har ansvaret for en funktion i det daglige, også har ansvaret, når der sker en alvorlig hændelse. Ansvaret omfatter også at planlægge, hvordan man vil opretholde og videreføre funktionerne, hvis der indtræffer en ekstraordinær hændelse. Ansvaret for cyber- og informationssikkerheden og dermed opgaven med at beskytte vores samfundskritiske infrastruktur er derfor delt mellem de myndigheder, som har ansvaret for de samfundskritiske sektorer, fx transport-, sundheds- og finanssektoren. Med Forsvarsforliget 2018-2023 sker der en væsentlig styrkelse af Center for Cybersikkerheds evne til bistå de sektoransvarlige myndigheder.

Den sektorvise ansvarsfordeling sikrer, at tiltagene tager højde for den enkelte sektors kendetegn og modenhed i forhold til cyber- og informationssikkerhed. Samtidig nødvendiggør sektoransvaret, at der er en central koordinering, både mellem sektorministerierne og mellem myndigheder med et tværgående ansvar. Det er afgørende, at staten fastsætter de overordnede strategiske rammer på cyber- og informationssikkerhedsområdet og understøtter

> **Danmark skal være stærkere repræsenteret i internationale drøftelser om cybersikkerhed og styring af internettet**

arbejdet hermed i de samfundskritiske sektorer. Til at understøtte og bistå den enkelte sektor i arbejdet med at opbygge den nødvendige cyber- og informationssikkerhed oprettes en midlertidig task force med deltagelse af Digitaliseringsstyrelsen, Center for Cybersikkerhed og Politiets Efterretningstjeneste.

For at imødekomme behovet for hurtigt at tilpasse indsatsen på cyber- og informationssikkerhedsområdet til den løbende udvikling i trusselsbilledet er der behov for at styrke den nationale tværgående koordinering på området. Derfor nedsætter regeringen Den nationale styregruppe for cyber- og informationssikkerhed. Øget koordinering og videndeling på området skal skabe bedre sammenhæng mellem de operationelle tiltag i de enkelte sektorer og den overordnede strategiske tilgang til cyber- og informationssikkerhed.

Regeringen ønsker desuden at fortsætte samarbejdet med eksperter fra den offentlige og den private sektor og derfor omlægges Dialogforum for informationssikkerhed til et advisory board med eksperter på området, som skal levere input til implementeringen og opfølgningen på cyberstrategien og dens initiativer.

Styrket internationalt engagement

I de kommende år vil cyberområdet være et af de mest prioriterede sagsområder i EU, og EU-kommissionen har blandt andet fremlagt en omfattende cyberpakke. Cyberområdet vil have tværgående betydning for en lang række sektorområder, såsom erhvervspolitik, energi- og forsyningssikkerhed, telekommunikation, forsvar, retsområdet samt offentlig og privat digitalisering. Regeringen vil derfor øge Danmarks engagement i det internationale samarbejde. Danmark skal være stærkere repræsenteret i drøftelser i EU-, NATO- og FN-sammenhænge om cybersikkerhed og styring af internettet, når drøftelserne har direkte betydning for danske borgere, virksomheder og myndigheder.

Regeringen vil også bringe Danmarks tech-ambassadør i spil på cyberområdet som led i en styrket dialog med de store, multinationale teknologivirksomheder og det øvrige tech-miljø om cyber- og informationssikkerhed, herunder dataetik og databeskyttelse. Regeringen vil ligeledes styrke cyberdiplomatiet ved at etablere en cyberkoordinator-funktion i Udenrigsministeriet, som skal styrke Danmarks engagement i det internationale samarbejde om cybersikkerhed.

Derudover iværksættes en indsats for styrket eksportkontrol med cyberovervågningsudstyr. Der fokuseres på at sikre klarere regler og kompetent vejledning fra myndighederne, således at virksomhederne tør satse på eksport og derigennem opbygge en stærk dansk cyberindustri, der samtidig kan bidrage til et styrket dansk cyberberedskab.

Regeringens initiativer – Fælles indsats

Initiativ 3.1: Sektorvise delstrategier og decentrale cybersikkerhedsenheder

For at opbygge stærkere decentral kapabilitet på cyber- og informationssikkerhedsområdet, oprettes der for hver af de samfundskritiske sektorer en sektorenhed, der kan bidrage til gennemførelsen af sektorvise trusselsvurderinger, overvågning, beredskabsøvelser, sikkerhedsopbygning, vidensdeling, vejledning mv. Endvidere skal der i 2018 for hver af de samfundskritiske sektorer udarbejdes en sektorspecifik strategi i forlængelse af den nationale strategi.

- **Initiativ 3.1a:** Cyber- og informationssikkerhedsstrategi for energisektoren
- **Initiativ 3.1b:** Cyber- og informationssikkerhedsstrategi for sundhedssektoren
- **Initiativ 3.1c:** Cyber- og informationssikkerhedsstrategi for transportsektoren
- **Initiativ 3.1d:** Cyber- og informationssikkerhedsstrategi for telesektoren
- **Initiativ 3.1e:** Cyber- og informationssikkerhedsstrategi for finanssektoren
- **Initiativ 3.1f:** Cyber- og informationssikkerhedsstrategi for søfartssektoren

Initiativ 3.2: Tværgående indsats for at understøtte samfundskritiske sektorers cyber- og informationssikkerhed

Der etableres en tværministeriel taskforce bestående af eksperter fra Center for Cybersikkerhed, Digitaliseringsstyrelsen og Politiets Efterretningstjeneste, som i en overgangsfase, gennem rådgivning og fælles tiltag, skal bistå de samfundskritiske sektorer med udformning af sektorstrategierne, bistå i etableringen af de decentrale cybersikkerhedsenheder og erfaringsudveksling samt udarbejde vejledninger for sektorernes arbejde med etablering af beredskabsplaner på informationssikkerhedsområdet.

Initiativ 3.3: Styr på leverandører af outsourcet it

For at øge it-sikkerheden og forsyningssikkerheden for myndighedernes samfundskritiske it-systemer indføres der skærpede krav til alle offentlige myndigheder om brug af tilstrækkelige sikkerheds- og styringsbestemmelser i fremtidige kontrakter for samfundskritiske it-systemer samt til myndighedernes styring af disse.

Initiativ 3.4: Styrket national koordinering

Den strategiske koordinering på cyber- og informationssikkerhedsområdet skal styrkes. Derfor oprettes "Den nationale styregruppe for cyber- og informationssikkerhed". Styregruppen får til ansvar at følge op på udmøntningen af strategien for cyber- og informationssikkerhed, iværksætte supplerede initiativer og analyser og løbende drøfte den nationale policy på cyber- og informationssikkerhedsområdet. Dialogforum for informationssikkerhed omlægges til et advisory board med eksperter på området, som skal levere input til implementeringen og opfølgningen på cyberstrategien og dens initiativer.

Initiativ 3.5: Styrket internationalt engagement

Regeringen vil styrke Danmarks internationale engagement ved at udstationere to cyber-attachéer på EU-repræsentationen i Bruxelles med henblik på at styrke Danmarks tværgående interessevaretagelse. Samtidig styrker regeringen tech-ambassadørens setup i Silicon Valley med en rådgiver dedikeret til cyber- og informationssikkerhed og styrker cyberdiplomatiet med en international cyberkoordinator i Udenrigsministeriet. Danmark vil desuden deltage i "NATO Cooperative Cyber Defence Center of Excellence" i Tallinn og i "European Centre of Excellence for countering hybrid threats" i Helsinki. Herudover øges indsatsen indenfor eksportkontrol med cyberovervågningsudstyr med henblik på at sætte danske virksomheder i stand til at navigere indenfor dette, samtidig med at dansk udviklet teknologi ikke bruges imod nationen af ondsindede aktører.

Initiativ 3.6: Tilstandsmåling af cyber- og informationssikkerhed

Der er behov for jævnligt at foretage en national analyse af cyber- og informationssikkerhedssituationen med henblik på at vurdere, om de iværksatte tiltag har den ønskede effekt og imødegår udviklingen i trusselsbilledet. Analysen skal anlægge såvel et bredt som et dybdegående blik på cyber- og informationssikkerheden i Danmark, herunder trusler, risici, beskyttelsesniveau, iværksatte foranstaltninger, organisering, sammenhænge mellem sektorer mv.

Initiativ 3.7: Overblik over beskyttelsesværdig information

Med henblik på at beskytte informationer af betydning for den nationale sikkerhed og styrke arbejdet med vurdering af informationssikkerhedsrisici iværksættes en indsats, der har til formål at skabe det fornødne overblik over beskyttelsesværdig information. Overblikket skal anvendes til at fastlægge konkrete klassifikations- og sikkerhedsniveauer, såvel myndighedsspecifikt som i forhold til den overordnede samfundsmæssige betydning af informationer.

Initiativ 3.8: Informationssikkerhedsarkitektur

Med henblik på at støtte myndighederne i at udvikle it-løsninger, der øger myndighedernes evne til at sikre fortrolighed, integritet, tilgængelighed og robusthed af systemer og -tjenester, udarbejdes en fællesoffentlig arkitektur for informationssikkerhed bestående af principper, standarder, fælleskomponenter og vejledninger.

Initiativ 3.9: National og international indsats for dataetik og persondatabeskyttelse

Regeringen vil styrke den dataetiske indsats både nationalt, i forhold til håndteringen af data i danske virksomheder, og internationalt. På nationalt niveau udarbejdes virksomhedsrettet informations- og vejledningsmateriale om reglerne for bl.a. ansvar, ejerskab og rettigheder ved anvendelse af data. Der er endvidere nedsat en ekspertgruppe med repræsentanter fra erhvervslivet, som skal udarbejde anbefalinger for dataetik. Regeringen vil desuden lancere en særskilt strategi om beskyttelse af danskernes personoplysninger. På internationalt niveau vil regeringen udpege dataetik og databeskyttelse som fokusområder for Danmarks tech-ambassadør i Silicon Valley, som led i en styrket dialog med de store, multinationale teknologivirksomheder.

Appendix

Ansvar og roller ved myndigheders arbejde med cyber- og informations-sikkerhed

Arbejdet med cyber- og informationssikkerhed er baseret på sektoransvarsprincippet. Det betyder, at den myndighed, der har ansvaret for en opgave til dagligt bevarer ansvaret under en hændelse. Det gælder både i det daglige beredskab, under hændelser og ved genopretning efter hændelser.

Generelle principper for det nationale krisestyringssystem i Danmark

Kilde: National Beredskabsplan, 6. udgave

Sektoransvarsprincippet
Den myndighed, der har ansvaret for en opgave til daglig, bevarer ansvaret for opgaven under en større ulykke eller katastrofe.

Lighedsprincippet
De procedurer og ansvarsforhold, der anvendes i dagligdagen, anvendes i videst muligt omfang også i krisestyringssystemet.

Nærhedsprincippet
Beredskabsopgaverne bør løses så tæt på borgerne som muligt og dermed på det lavest egnede, relevante organisatoriske niveau.

Samarbejdsprincippet
Myndighederne har et selvstændigt ansvar for at samarbejde og koordinere med andre myndigheder og organisationer, både vedrørende beredskabsplanlægning og krisestyring.

Handlingsprincippet
I en situation med uklare eller ufuldstændige informationer er det mere hensigtsmæssigt at etablere et lidt for højt beredskab end et lidt for lavt beredskab. Samtidig skal der hurtigt kunne ændres på beredskabet i nedadgående retning for at undgå ressourcespild.

Sektoransvarsprincippet

Kilde: Præcisering af sektoransvar for ministerier og styrelser, National sårbarhedsrapport, 2006

Sektoransvarsprincippet indebærer bl.a., at

1. Alle ministre skal sikre et forsvarligt beredskab inden for eget ressort
2. Sektoransvaret omfatter alle kritiske funktioner og opgaver, som er pålagt lovgivningsmæssigt, politisk eller administrativt
3. Myndighedernes beredskabsplanlægning skal bygge på en løbende og systematisk risikovurderingsproces, som er forankret i ledelsen
4. Myndighederne skal løbende overvåge risikobilledet inden for egen sektor

2. Ansvar og roller ved hændelser af betydning for cyber- og informationssikkerheden

2.1. Hændelse inden for en sektor

Den enhed (myndigheder, virksomheder og organisationer), der har ansvaret for en opgave til daglig, har fortsat ansvaret, når der opstår en cyberhændelse. Enheden skal sikre, at den i den forbindelse får den aftalte bistand fra eventuelle driftsleverandører. Derudover kan enheden få bistand fra de decentrale cybersikkerhedsenheder. Det er enhedens ansvar at aktivere denne bistand, forestå den indledende hændelseshåndtering og, afhængigt af hændelsens omfang, at indberette denne til kompetente myndigheder og Center for Cybersikkerhed. Det er ligeledes den ansvarlige myndighed, virksomhed eller organisation, der som udgangspunkt varetager evt. ekstern kommunikation om hændelsen.

2.2. Større, tværgående hændelser

Ved større cyberhændelser, der påvirker flere sektorer, kan National Operativ Stab (NOST), hvor bl.a. Rigspolitiet, PET og FE/Center for Cybersikkerhed er faste medlemmer, aktiveres.

Sektoransvarsprincippet indebærer imidlertid fortsat, at det er de sektoransvarlige myndigheders ansvar at sikre et overblik over hændelsens omfang og at rapportere dette til relevante myndigheder, herunder CFCS og NOST, hvis denne er etableret, ligesom det er de berørte myndigheder, virksomheder og organisationers ansvar at håndtere hændelsen og dens følger. Afhængig af hændelsens omfang og karakter kan Center for Cybersikkerhed i den forbindelse assistere de ramte enheder med imødegåelsen af hændelsen. Center for Cybersikkerhed kan således foretage tekniske undersøgelser af cyberangreb med henblik på dels at stoppe den enkelte hændelse, dels at klarlægge eventuelle angrebsmetoder eller sårbarheder, således at samfundets beskyttelse mod tilsvarende situationer kan styrkes. Disse undersøgelser udføres i et tæt samarbejde med den udsatte enhed.

Ved langt de fleste større cyberangreb vil der være behov for både efterforskning og it-sikkerhedstekniske undersøgelser. Der er derfor etableret et tæt samarbejde mellem politiet (herunder PET) og Center for Cybersikkerhed, som indebærer, at der sker en gensidig orientering ved større cyberhændelser,

herunder forsætlige angreb, ligesom der ofte vil være et operativt samarbejde i forbindelse med konkrete hændelser.

2.3. Kommunikation

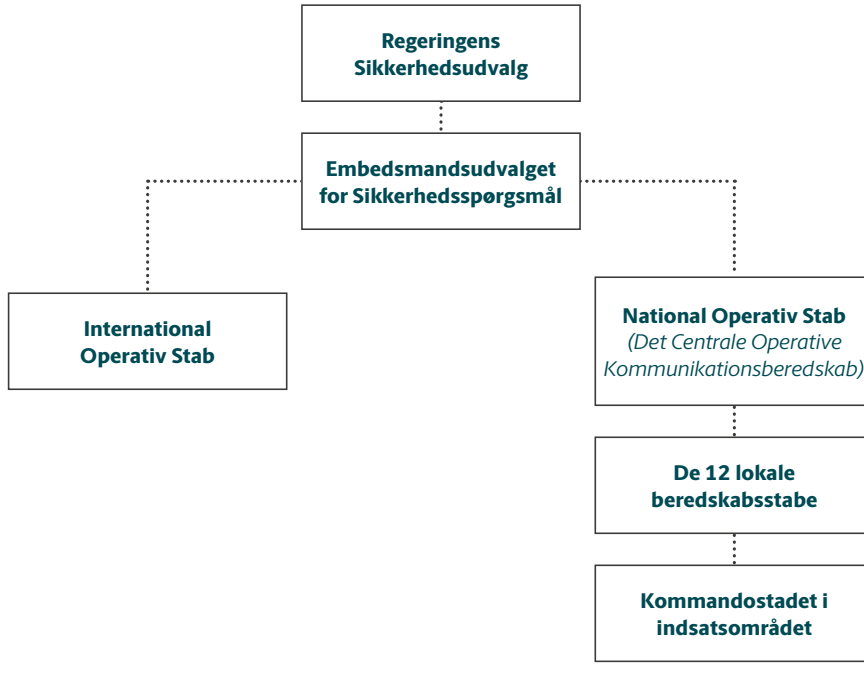
Ekstern kommunikation ved mindre hændelser, der ikke berører flere sektorer, håndteres som udgangspunkt af den sektoransvarlige myndighed. Kommunikation om cybertrusler og det aktuelle situationsbillede samt krisekommunikation i forbindelse med cyberhændelser i øvrigt varetages af Center for Cybersikkerhed i samarbejde med den relevante sektoransvarlige myndighed.

I tilfælde af en større, tværgående hændelse vil der skulle ske en koordination af kommunikationen. Via myndighedssamarbejdet inden for NOST koordinerer Det Centrale Operative Kommunikationsberedskab (DCOK) kommunikationen. DCOK har således til opgave at sikre hurtig videregivelse af relevante og koordinerende informationer til offentligheden, herunder medierne. DCOK har endvidere til opgave – om fornødent – at etablere enheder, hvor borgere kan få yderligere oplysninger vedrørende konkrete hændelser.

2.4. Genopretning efter en cyberhændelse

Den berørte enhed (myndighed, virksomhed eller organisation) forestår med udgangspunkt i sin beredskabsplan selv genopretning af såvel den forretningsmæssige drift som it-driften. Den berørte enhed kan i arbejdet blive støttet af offentlige eller private leverandører på området og eventuelt af de decentrale cybersikkerhedsenheder i de enkelte sektorer.

Figur 1
Det nationale krisestyringssystem



Kilde: Krisestyring i Danmark, Beredskabsstyrelsen, 2015

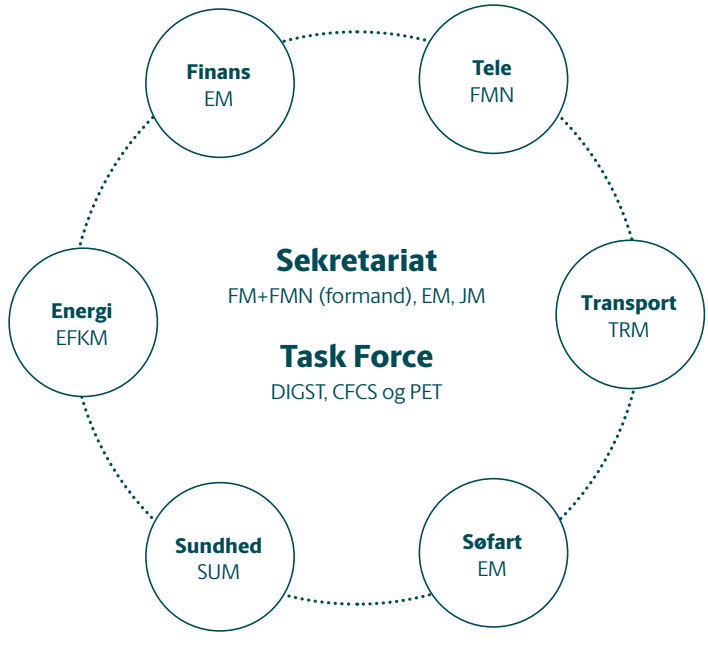
3. Løbende koordinering

Det løbende arbejde med cyber- og informationssikkerhed skal ske med tæt koordinering og vidensdeling mellem relevante myndigheder. Derfor igangsættes en række initiativer, som understøtter arbejdet i sektorer, myndigheder og virksomheder, og som sikrer en tættere national koordination på området, særligt ift. det forebyggende arbejde med it-sikkerhed.

Med strategien sættes der fokus på kravet om, at de samfundskritiske sektorer skal opbygge en dedikeret cyber- og informationssikkerhedsenhed, der kan bidrage til sektorvise trusselsvurderinger, sårbarhedsvurderinger, beredskabsøvelser, sikkerhedsopbygning, videndeling, vejledning mv.

For at styrke den strategiske koordination og implementering af strategien nedsættes en national styregruppe for cyber- og informationssikkerhed, hvor arbejdet i de enkelte sektorer knyttes sammen med den nationale indsats på området.

Med kravet om sektorstrategier og dedikerede cyber- og informationssikkerhedsenheder i de enkelte sektorer sikres en tættere tværgående koordination inden for den enkelte sektor samt imellem sektorerne og nationale indsatser. Der etableres en task force med deltagelse af Digitaliseringsstyrelsen, Center for Cybersikkerhed og Politiets Efterretningstjeneste, der gennem rådgivning og fælles tiltag skal bistå sektorerne med etablering af cyber- og informationssikkerhedsenhederne og udarbejdelse af de sektorspecifikke strategier.



Figur 2
Styregruppe for national koordinering og opfølgning på cyber- og informationssikkerhedsstrategien

Myndigheder, der leverer information, rådgivning og vejledning på cyber- og informationssikkerhedsområdet

Center for Cybersikkerhed
CFCS er national it-sikkerhedsmyndighed og varetager en række opgaver af forebyggende og afhjælpende karakter, herunder bl.a. rådgivning. CFCS' netsikkerhedstjeneste kan bidrage til at opdage og varsle om avancerede cyberangreb hos tilsluttede myndigheder og virksomheder. CFCS varsler relevante myndigheder og virksomheder om konkrete cybertrusler, ligesom centeret udarbejder nationale og sektorspecifikke situationsbilleder og trusselsvurderinger.

Politiet
Politiet har til opgave at forebygge og efterforske it-relateret kriminalitet, og bringe kriminalitet til ophør. Politiet har desuden det koordinerende ansvar ved større, tværgående hændelser.

Politiets Efterretningstjeneste
PET er national sikkerhedsmyndighed og kan i den forbindelse bl.a. yde rådgivning og bistand til offentlige myndigheder og private i sikkerhedsspørgsmål, herunder for så vidt angår den menneskelige faktor i informationssikkerhed tillige med fysiske sikring.

Digitaliseringsstyrelsen
Digitaliseringsstyrelsen understøtter informationssikkerheden i den offentlige sektor og varetager en række borgerrettede informationsopgaver samt har ansvaret for at koordinere implementeringen af strategien i samarbejde med FMN.

Erhvervsstyrelsen
Erhvervsstyrelsen udarbejder information, vejledning og værktøjer til at styrke det brede erhvervslivs arbejde med it-sikkerhed og ansvarlig datahåndtering.

4. Myndigheder med et tværgående ansvar for cyber- og informationssikkerhed

Myndighedernes arbejde med cybersikkerhed understøttes af bistand, information, vejledning og rådgivning fra myndigheder med en tværgående og koordinerende funktion på området. Det er myndighedernes ansvar aktivt at efterspørge den bistand, der vurderes relevant.

4.1. Center for Cybersikkerhed

Center for Cybersikkerhed blev dannet i 2012 for at styrke beskyttelsen mod cyberangreb mv. Jf. FE-loven er Forsvarets Efterretningstjeneste bl.a. national it-sikkerhedsmyndighed, og denne funktion varetages af Center for Cybersikkerhed.

På det proaktive område tilbyder Center for Cybersikkerhed at rådgive statslige myndigheder om cybersikkerhed, f.eks. ved indkøb af it-udstyr eller design af nye it-systemer. Desuden udgiver centeret vejledninger om håndtering af cybersikkerhedsmæssige udfordringer. CFCS' trusselsvurderingsenhed udarbejder nationale og sektorspecifikke situationsbilleder og trusselvurderinger.

På det reaktive område har blandt andet statslige myndigheder mulighed for at blive tilsluttet centerets netsikkerhedstjeneste, der sikrer, at myndighedens internetkommunikation løbende monitoreres for skadelig trafik ved hjælp af særlige alarmenheder. Endvidere kan statslige myndigheder døgnet rundt kontakte netsikkerhedstjenesten, hvis der konstateres mulige cyberangreb, hvorefter netsikkerhedstjenesten kan yde assistance, f.eks. ved udsendelse af et Rapid Response Team.

Regeringen har besluttet, at alle statslige myndigheder skal rapportere større it-sikkerhedshændelser i deres egne it-systemer til Center for Cybersikkerhed, således at netsikkerhedstjenesten har det bedst mulige overblik over den aktuelle sikkerhedssituation på den danske del af internettet.

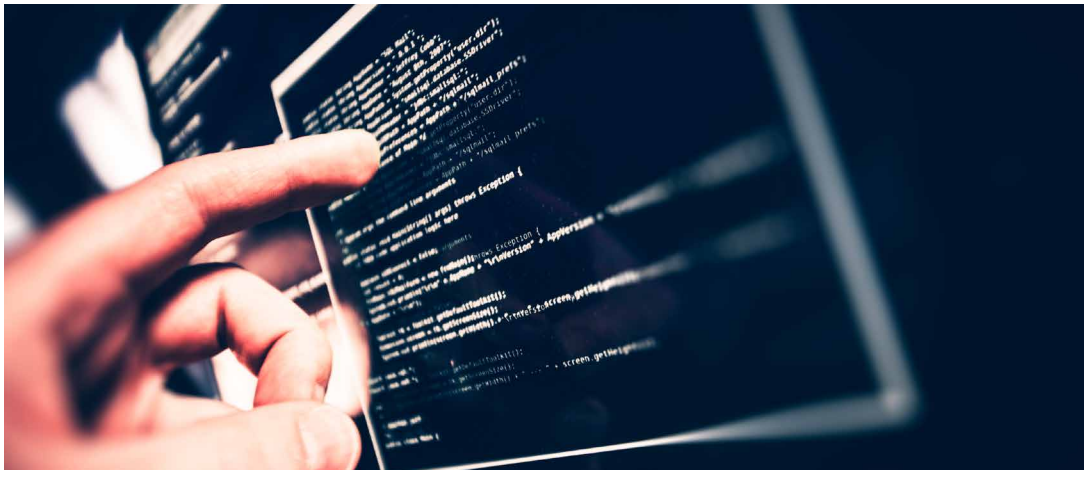
“Myndighederne understøttes af bistand, information, vejledning og rådgivning fra myndigheder med en tværgående og koordinerende funktion

Center for Cybersikkerhed udgiver jævnligt situationsbilleder og trusselsvurderinger. Uklassificerede situationsbilleder og trusselsvurderinger kan findes på Center for Cybersikkerheds hjemmeside, www.cfcs.dk. Klassificerede trusselsvurderinger og varslinger om konkrete cybersikkerhedshændelser distribueres direkte til de berørte myndigheder.

Med forsvarsforliget 2018-2023 sker der en væsentlig styrkelse af Center for Cybersikkerheds evne til at bistå de sektoransvarlige myndigheder. Styrkelsen af Center for Cybersikkerhed vil både omfatte centrets rådgivende og forebyggende rolle og indsatsen i forhold til at opdage og varsle om konkrete hændelser inden for samfundsvigtige sektorer. Det sker bl.a. ved etableringen af et nyt døgnbemandet nationalt cybersituationscenter som vil skulle operationalisere oplysninger fra efterretningskilder, indberetninger mv. og dermed skabe et nationalt situationsbillede over den aktuelle sikkerhedstilstand for samfundsvigtige digitale netværk.

4.2. Politiets Efterretningstjeneste (PET)

PET har i medfør af PET-loven til opgave at forebygge, efterforske og modvirke trusler og handlinger, der udgør eller vil kunne udgøre en fare for Danmark som et selvstændigt, demokratisk og sikkert samfund. Ansvarsområdet for PET er forbrydelserne omhandlet i straffelovens kapitel 12 (om forbrydelser mod statens selvstændighed og sikkerhed) og 13 (om forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme m.v.), herunder forbrydelser der i den forbindelse er rettet mod informations- og



kommunikationssystemer, eller som indebærer anvendelse af informations- og kommunikationsteknologi.

PET skal gennem sin virksomhed medvirke til, at trusler af den nævnte karakter identificeres og håndteres så tidligt og effektivt som muligt.

PET er endvidere national sikkerhedsmyndighed og rådgiver i den forbindelse om den fysiske beskyttelse af følsom information, herunder om sikkerhedsmæssig håndtering af medarbejdere med fysisk adgang til information og informationssystemer, herunder gennemførsel af sikkerhedsundersøgelser og -godkendelser. PET varetager endelig funktionen som it-sikkerhedsmyndighed på Justitsministeriets område.

4.3. Politiet

Politiet har i medfør af lov om politiets virksomhed (politiloven) til opgave at forebygge og efterforske strafbare forhold og bringe strafbar virksomhed til ophør, herunder sager om it-relateret kriminalitet.

Med henblik på en styrkelse af håndteringen af it-relateret kriminalitet har Rigspolitiet i 2014 etableret et nationalt Cyber Crime Center (NC3). Centret har – med forbehold for de opgaver, der varetages af PET – det overordnede ansvar for at sætte retning for politiets opgavevaretagelse vedrørende bl.a. kriminalitet, der retter sig imod it-systemer, og kriminalitet, der begås under anvendelse af it.

Politiets kompetence omfatter alle strafbare forhold, der er undergivet dansk straffemyndighed. Dette gælder ligeledes handlinger, der foretages uden for den danske stat, når handlingerne krænker den danske stats selvstændighed, sikkerhed, forfatning eller offentlige myndigheder, eller når virkningen af de strafbare handlinger er tilsigtet at skulle indtræde her i landet.

Politiet har desuden i medfør af beredskabsloven det koordinerende ansvar for den samlede indsats ved større skader, herunder også for så vidt angår bl.a. varsling mv.

2017/18:29

April 2018

Finansministeriet
Christiansborg Slotsplads 1
1218 København K
Tlf.: +45 3392 3333
E-mail: fm@fm.dk

ISBN 978-87-93635-45-6 (pdf version)
ISBN 978-87-93635-36-4 (trykt version)

Design: e-Types
Foto: Ritzau Scanpix, Colourbox,
Johnér og Pexels
Tryk: Rosendahls

Publikationen kan hentes på
fm.dk /regeringen.dk

Finansministeriet
Christiansborg Slotsplads 1
1218 København K
Tlf.: +45 3392 3333