National strategi for cyber- og informationssikkerhed

Øget professionalisering og mere viden

December 2014

Regeringen

INFORMATIONSSIKKERHED OG CYBERSIKKERHED

I denne strategi anvendes to begreber:

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.

Begreberne er yderligere beskrevet i bilag 2.

National strategi for cyber- og informationssikkerhed

Øget professionalisering og mere viden

December 2014

Regeringen

Indhold

Forord

Regeringen har siden sin tiltræden haft fokus på at styrke cyber- og informationssikkerhedsindsatsen. Det fremgår således af regeringsgrundlaget "Et Danmark, der står sammen", at *"regeringen vil med respekt for retssikkerheden og den personlige frihed styrke beskyttelsen mod cyberangreb"*. I Danmark skal borgere og virksomheder kunne have tillid til, at varetagelsen af vigtige funktioner i samfundet sker på en effektiv og sikker måde.

Flere og flere områder digitaliseres, hvilket er afgørende for den videre udvikling af velfærdssamfundet. Fremadrettet er det tilsvarende afgørende, at cyber- og informationssikkerhedsarbejdet professionaliseres og løbende udvikles. Den digitale infrastruktur skal beskyttes. Det forudsætter, at cyber- og informationssikkerhed sættes på den ledelsesmæssige dagsorden og prioriteres. Den seneste tid har budt på en række nye udfordringer og trusler, fx er det i enkelte tilfælde lykkedes hackere at forstyrre driften af vigtige funktioner i samfundet, eller de har været i stand til at tilgå følsomme og værdifulde oplysninger.

Forsvarets Efterretningstjeneste vurderer, at forekomsten af it-relaterede trusler mod private borgere, virksomheder og offentlige myndigheder er stigende. Udefrakommende cyberangreb mod digitale systemer er over en kortere årrække blevet mere udbredte og mere avancerede. Samtidig vurderes det, at staten i nogle tilfælde kan stå over for en udfordring, når det kommer til outsourcing af dele af den infrastruktur, som samfundsvigtige funktioner er afhængige af.

Danmark skal både have en stærk forebyggende og en stærk reaktiv beskyttelse mod disse trusler. Derfor er det vigtigt, at der i samfundet er en bredere viden om og forståelse for de trusler, vi står over for. Denne strategi for en styrket cyber- og informationssikkerhed sætter derfor fokus på behovet for mere viden på området og en professionalisering af det daglige arbejde med cyber- og informationssikkerhed i de statslige myndigheder samt på cyber- og informationssikkerheden i telesektoren og energisektoren.

Det er centralt for forankringen af dette arbejde, at indsatsen integreres i myndighedernes eksisterende arbejde, så professionaliseringen af cyber- og informationssikkerhedsarbejdet sker i tæt samspil med myndighedernes faglige viden om de områder, som de hver især har ansvaret for.

Med denne strategi tager regeringen et væsentligt skridt til at opretholde og styrke tilliden hos virksomheder og borgere til, at Danmark fortsat er et sikkert land at investere og anvende digitale tjenester i. Udviklingen på det digitale område vil fortsætte, og derfor er det afgørende, at der løbende arbejdes med fortsat at styrke indsatsen på området. På den baggrund agter regeringen at opdatere denne strategi allerede i slutningen af 2016 for en ny periode. I forbindelse med opdateringen vil regeringen indlede en bred dialog med relevante organisationer, virksomheder og forskningsverdenen for at inddrage forskellige synspunkter og viden om, hvad der vil være til gavn for samfundet i det videre arbejde.

Nicolai Wammen
Forsvarsminister

Bjarne Corydon
Finansminister

Martin Lidegaard
Udenrigsminister

Mette Frederiksen
Justitsminister

Sofie Carsten Nielsen
Uddannelses- og forskningsminister

Henrik Sass Larsen
Erhvervs- og vækstminister

Rasmus Helveg Petersen
Klima-, energi- og bygningsminister

Benny Engelbrecht
Skatteminister

Resumé

Med denne strategi tages en række initiativer til styrkelse af cyber- og informationssikkerheden i Danmark. Initiativerne falder inden for seks områder.

Professionalisering og styrket it-tilsyn
Arbejdet med informationssikkerhed professionaliseres, og it-tilsynet i de statslige myndigheder styrkes. Desuden skabes yderligere dialog mellem private og offentlige aftagere og relevante uddannelses- og forskningsinstitutioner på området.

Klare krav til leverandører
Statslige myndigheder skal fremover arbejde mere systematisk med at stille sikkerhedsmæssige krav i forbindelse med udbud og ved indgåelse af kontrakter på it-området. Desuden skal der ske løbende opfølgning på den sikkerhedsmæssige leverandørstyring i staten.

Styrket cybersikkerhed og mere viden på området
Viden om cybertrusler skal i højere grad indgå i myndighedernes og virksomhedernes arbejde med cyber- og informationssikkerhed. Der etableres en enhed for vurdering af cybertrusler og tages initiativ til systematisk undersøgelse af større cybersikkerhedshændelser. Endvidere etableres et virksomhedsråd for it-sikkerhed.

Robust infrastruktur i energisektoren og telesektoren
Regeringen styrker cyber- og informationssikkerheden i telesektoren og i energisektoren.

Danmark som stærk international medspiller
Regeringen styrker arbejdet med at fremme Danmarks holdning i internationale samarbejder om cyber- og informationssikkerhed. Endvidere prioriterer regeringen nordisk samarbejde om forskning og uddannelse i cyber- og informationssikkerhed.

Stærk efterforskning og klar information til borgere, virksomheder og myndigheder
Regeringen vil sikre en højere sikkerhedsbevidsthed blandt borgerne i Danmark, og der indføres en række konkrete borgerrettede sikkerhedstiltag. Der udvikles et frivilligt sikkerhedstjek for virksomheder. Ydermere udvides den efterforskningsmæssige kapacitet på cybersikkerhedsområdet og politiets rådgivning om informationssikkerhed styrkes.

1.0 Indledning

1.1 En stærk og sammenhængende sikkerhed

Danmark har igennem en årrække oplevet en omfattende digital udvikling. Digitalisering er et globalt fænomen, der med stor hastighed forandrer alle niveauer i samfundet. Digitaliseringen påvirker i høj grad kommunikationen mellem borgere, virksomheder og det offentlige, og hvordan vi indretter og organiserer vores samfund.

Digitaliseringen er i dag ikke længere et valg, men et vilkår. Danske virksomheder anvender digital teknologi i både produktion og interne processer – og i tiltagende grad i deres produkter. I de senere år har det offentlige Danmark samtidig gennemført en række digitaliseringsstrategier med fokus på digital forvaltning, effektivisering og samarbejde, digital service og digital velfærd. Den effektivisering og den innovation, som digitaliseringen rummer, er afgørende for Danmarks konkurrenceevne og velfærd.

Fordi digitaliseringen er så vigtig en del af den offentlige opgavevaretagelse og for samfundets funktion i øvrigt, lægger regeringen vægt på, at indsatsen på cyber- og informationssikkerhedsområdet løbende forbedres. Regeringen vil med denne strategi hæve niveauet for det statslige cyber- og informationssikkerhedsarbejde ved at arbejde systematisk efter sikkerhedsstandarden ISO27001 og med trusselvurderinger samt ved at understøtte og styrke ministeriernes it-tilsyn med de statslige myndigheder. Det er samtidig vigtigt, at der foretages en stærk sikkerhedsmæssig styring af eksterne leverandører, fordi en stor del af den statslige it er outsourcet. Endvidere skal der foretages en sikkerhedsmæssig risikovurdering af it-projekter ved, at dette indarbejdes i den fællesstatslige it-projekt og den fællesstatslige programmodel.

Disse tiltag skal sikre, at myndighederne professionaliserer deres daglige arbejde med informationssikkerhed og skabe grundlaget for, at der løbende etableres en øget robusthed mod cyberangreb. Samtidig vil regeringen fortsat styrke beskyttelsen mod cyberangreb. Med strategien tages der en række initiativer til at opnå øget viden om trusler og til at foretage systematisk opsamling af erfaringer med cyberangreb.

Strategien er målrettet de statslige myndigheder, men den indeholder også en indsats målrettet virksomheder med infrastruktur af væsentlig samfundsmæssig betydning på energiområdet og teleområdet.

1.2 Udfordringen

Udfordringerne på cyber- og informationssikkerhedsområdet har både tekniske og mere konkrete og praktiske sider.

Manglende efterlevelse af sikkerhedsrutiner. En del af udfordringen er at få rustet de offentlige myndigheder til at indarbejde en systematisk stillingtagen til informationssikkerhed i myndighedernes daglige rutiner. Hvis myndighederne ikke prioriterer at få etableret de nødvendige informationssikkerhedsrutiner og foretager konkrete risikovurderinger af centrale systemer, så er der en risiko for, at myndighederne overser sikkerhedsmæssige mangler og sårbarheder.

Dynamisk udvikling på området. Truslerne på cyber- og informationssikkerhedsområdet er dynamiske. Det vil sige, at der løbende opstår nye trusler, som myndighederne skal reagere på. Der er ikke udsigt til, at den udvikling vil aftage i de kommende år, tværtimod. Indsatsen for at håndtere truslerne skal derfor løbende forbedres og fornys.

Cybertrusler. Forsvarets Efterretningstjeneste vurderer, at danske offentlige myndigheder, virksomheder og privatpersoner dagligt udsættes for forsøg på skadelige aktiviteter fra forskellige aktører via internettet. Alvorlige kompromitteringer mod offentlige myndigheder er stadig sjældne, men trusselsbilledet viser, at disse risici er stigende. Forsvarets Efterretningstjeneste vurderer, at de alvorligste cybertrusler mod Danmark kommer fra fremmede statslige aktører, der udnytter internettet til at spionere og forsøge at stjæle dansk intellektuel ejendom og forretningshemmeligheder såsom forretningsplaner, forskningsresultater, teknisk knowhow, budgetter og aftaler.

Insidertrusler. Den såkaldte insidertrussel udgør endvidere en væsentlig udfordring. Eksempelvis er det en trussel, at medarbejdere bevidst eller ubevidst bryder sikkerhedspolitikker på deres arbejdsplads. Her er særligt den ubevidste trussel en udfordring – fx at holde døren for ukendte gæster, download af usikre programmer mv. Hvis medarbejdere ikke efterlever fastlagte sikkerhedspolitikker, stiger risikoen for, at uvedkommende kan få adgang til interne netværk og dermed fortrolige informationer.

Leverandørstyring. Staten står desuden over for en række særlige trusler i forbindelse med outsourcet it-drift. Statslige myndigheder skal derfor blive dygtigere til at følge op på sikkerhedsniveauet hos eksterne leverandører, hvilket blandt andet det alvorlige angreb mod it-leverandøren CSC i 2012 har vist behovet for.

1.3 Stærkere myndighedsindsats

Regeringen har allerede iværksat en række tiltag til styrkelse af cybersikkerheden i staten og følger myndighedernes arbejde på området. Først og fremmest er indsatsen blevet forstærket i myndigheder med særlige opgaver på området.

Regeringen har blandt andet oprettet Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste. Centrets hovedopgave er at understøtte, at sikkerheden styrkes mod udefrakommende trusler i de systemer og den infrastruktur, som samfundsvigtige funktioner er afhængige af.

Regeringen har endvidere etableret Digitaliseringsstyrelsen for at samle aktiviteter vedrørende digitaliseringen i staten. Digitaliseringsstyrelsen arbejder for at sikre en professionel og sammenhængende styring og udvikling af den fællesoffentlige digitale infrastruktur (NemID, NemKonto, NemLog-in, Digital Post og borger.dk). Styrelsen rådgiver også de statslige myndigheder om styring af informationssikkerhed efter principper, som er obligatoriske i staten.

Politiet har desuden etableret Nationalt Cyber Crime Center (NC3), som har til opgave at forebygge, efterforske og opklare it-kriminalitet på eller via internettet.

Der er med denne stærke myndighedsindsats etableret et godt grundlag for, at myndigheder og virksomheder med systemer og infrastruktur af væsentlig betydning for samfundet kan tage yderligere skridt til at øge informationssikkerheden og cybersikkerheden. Som det fremgår af denne strategi, bygger det fremadrettede arbejde videre på en i forvejen styrket indsats.

1.4 Strategiske målsætninger

De overordnede målsætninger for regeringens arbejde med at styrke cyber- og informationssikkerhedsarbejdet er:

- Borgere og virksomheder skal have tillid til, at cyber- og informationssikkerheden i staten og blandt leverandører af samfundsmæssig væsentlig infrastruktur håndteres professionelt og betryggende. Indsatsen for at styrke cyber- og informationssikkerheden skal samtidig muliggøre en brugervenlig og effektiv udnyttelse af nye teknologiske muligheder.

- Der skal ske en styrket beskyttelse af vigtige samfundsfunktioner og af den nationale sikkerhed mod cyberangreb.

Sikkerhed i balance

De enkelte myndigheders indsats på informationssikkerhedsområdet skal ikke være ens. Indsatsen skal vægtes med udgangspunkt i en konkret vurdering mellem hensynene: *Sikkerhed, brugervenlighed og økonomi*. Det er væsentligt, at indsatsen er proportional med truslerne på det konkrete område. Der skal ikke arbejdes med sikkerhed for enhver pris. Sikkerhedstiltagene må ikke ske på bekostning af fx brugeroplevelsen og effektiviteten i en digital service, uden der er foretaget en konkret vurdering af, at sikkerhedsniveauet er nødvendigt. De enkelte myndigheder skal derfor arbejde risikobaseret med sikkerhed.

Til at understøtte målsætningen har regeringen udpeget seks strategiske indsatsområder med konkrete initiativer, som skal løfte samfundets informationssikkerhed og cybersikkerhed. Initiativerne danner grundlaget for, at der i samfundet løbende kan opretholdes et passende sikkerhedsniveau. De seks indsatsområder vil styrke den danske indsats i forhold til cyber- og informationssikkerhed væsentligt.

Professionalisering og styrket it-tilsyn
- At ministerierne arbejder systematisk og professionelt med informationssikkerhed og fører et stærkt it-tilsyn med egne statslige myndigheder.

Klare krav til leverandører
- At der stilles klare krav til cyber- og informationssikkerhed hos myndighedernes leverandører, og at der sker en løbende risikovurdering af og opfølgning på leverandørers it-sikkerhedsarbejde.

Styrket cybersikkerhed og mere viden på området
- At der sker en højnelse af den offentlige sektors cybersikkerhed, og at myndigheder og virksomheder har adgang til trusselbilleder og til avanceret viden om håndtering af sårbarheder.

Robust infrastruktur i energisektoren og telesektoren
- At der er et højt niveau af cyber- og informationssikkerhed i energisektoren og telesektoren.

Danmark som stærk international medspiller
- At danske myndigheder internationalt arbejder for at styrke cyber- og informationssikkerheden gennem aktiv deltagelse i relevante fora.

Stærk efterforskning og klar information til borgere, virksomheder og myndigheder
- At der er en stærk og kompetent efterforskning af it-kriminalitet, og at borgere og virksomheder får bedre forudsætninger for at tage ansvar for sikkerheden i eget udstyr og i egen adfærd på nettet.

Det er samtidigt væsentligt at pointere, at det ikke er muligt at garantere 100 pct. sikkerhed mod nedbrud, kompromitteringer og andre sikkerhedshændelser. Områdets dynamiske karakter indebærer, at arbejdet med cyber- og informationssikkerhed løbende skal udvikles og suppleres med nye tiltag. Myndigheder og leverandører skal arbejde risikobaseret. Det vil sige, at de hverken kan eller skal prioritere samtlige mulige tiltag for at øge sikkerheden. Myndigheder og leverandører skal ud fra løbende systematiske vurderinger og opfølgninger prioritere de indsatser, der giver størst sikkerhed i forhold til ressourceforbruget og i forhold til brugervenligheden af løsningerne.

1.5 Strategiens afgrænsning

Strategien fokuserer på statslige myndigheders cyber- og informationssikkerhedsarbejde. Med strategien iværksættes en koordineret, langsigtet indsats i staten. Der vil være tale om en indsats, som på forskellige sektorområder løbende skal udvikles og suppleres. Netop en professionalisering af det statslige arbejde med cyber- og informationssikkerhed har en central betydning for en række samfundsmæssigt centrale digitale infrastrukturer.

Strategien fokuserer desuden særligt på cyber- og informationssikkerhed i energisektoren og telesektoren, hvor private virksomheder ejer og understøtter en stor del af infrastrukturen. Begrundelsen herfor er, at teleinfrastrukturen er rygraden i samfundets kommunikation, og at energiinfrastrukturen leverer energi til samfundet og er en forudsætning for samfundsvigtige funktioner.

Sideløbende med strategiarbejdet er det som led i det fællesoffentlige samarbejde med kommuner og regioner aftalt, at informationssikkerhedsarbejdet skal styrkes yderligere med henblik på at sikre følsomme personoplysninger og et højt sikkerhedsniveau i den digitale infrastruktur i stat, kommuner og regioner. Regeringen forventer at styrke dette samarbejde i forbindelse med den næste fællesoffentlige digitaliseringsstrategi. Strategien udarbejdes i samarbejde mellem staten, kommunerne og regionerne og forventes lanceret i 2015. Informationssikkerhed vil være et særligt fokusområde i den næste fællesoffentlige digitaliseringsstrategi. Digitaliseringsstyrelsen vil endvidere sammen med de fællesoffentlige parter vurdere, om der i staten, kommuner og regioner er behov for yderligere indsats i forhold til implementering af ISO27001, når effekterne af initiativerne fra denne strategi kan vurderes.

På baggrund af de indledende erfaringer med cyber- og informationssikkerhedsstrategien agter regeringen ultimo 2016 at opdatere strategien. Dette vil ske på baggrund af en opfølgning på de igangsatte initiativer og en vurdering af, hvor det til den tid vil være særligt relevant at sætte ind med yderligere initiativer. Opdateringen vil således indbefatte andre relevante sektorer, fx finanssektoren. Opfølgningen er nærmere beskrevet i kapitel 8.

MÅLSÆTNING: EN STÆRK OG SAMMENHÆNGENDE SIKKERHED

- Borgere og virksomheder skal have tillid til, at cyber- og informationssikkerheden i staten og blandt leverandører håndteres professionelt og betryggende.
- Der skal ske en styrket beskyttelse af vigtige samfundsfunktioner og af den nationale sikkerhed mod cyberangreb.

INDSATSOMRÅDER

Professionalisering og styrket it-tilsyn	**Klare krav til leverandører**	**Styrket cybersikkerhed og mere viden på området**	**Robust infrastruktur i energisektoren og telesektoren**	**Danmark som stærk international medspiller**	**Stærk efterforskning og klar information til borgere, virksomheder og myndigheder**

INITIATIVER

1 Styrket arbejde med informationssikkerhed i staten. **2** Sikkerhedsmæssig risikovurdering i offentlige it-projekter. **3** Fællesoffentlig koordinering af informationssikkerhed. **4** Cyber- og informationssikkerhedsnetværk blandt uddannelses- og forskningsinstitutioner. **5** Styrket dialog mellem private og offentlige aftagere og de relevante uddannelses- og forskningsinstitutioner. **6** Kapacitet i Statens It til håndtering af cyberangreb.	**7** Sikkerhedsmæssige krav i udbud og ved indgåelse af kontrakter på it-området. **8** Løbende opfølgning på den sikkerhedsmæssige leverandørstyring.	**9** Cybertrusler skal indgå i grundlaget for myndighedernes risikoledelse fra 2015. **10** Etablering af enhed for vurdering af cybertrusler. **11** Analyse af statens forbindelser til internettet. **12** Analyse vedrørende styrkelse af sikker kommunikation i staten. **13** Enhed til undersøgelse af større cybersikkerhedshændelser. **14** SCADA-kompetencecenter i Center for Cybersikkerhed. **15** Etablering af Virksomhedsråd for It-sikkerhed.	**16** Styrkelse af net- og informationssikkerheden i samfundet. **17** Opgradering af kravene til cyber- og informationssikkerhed på energiområdet.	**18** Styrke det danske cyberdiplomati. **19** Fremme af Danmarks holdning i internationale samarbejder om cyber- og informationssikkerhed. **20** Nordisk samarbejde om forskning og uddannelse i cyber- og informationssikkerhed .	**21** Højere sikkerhedsbevidsthed blandt borgere. **22** Sikkerhedstjek for virksomheder. **23** Udbygning af Nationalt Cyber Crime Center. **24** Styrkelse af politiets rådgivning om informationssikkerhed. **25** Styrkelse af PET's kapacitet og kapabilitet på cyberområdet. **26** Online anmeldelsesplatform. **27** Blokering af stjålne identitetsoplysninger.

2.0 Professionalisering og styrket it-tilsyn

2.1 Målsætning for området

Der er behov for at styrke og professionalisere arbejdet med informationssikkerhed i staten. Derfor skal ministerierne arbejde professionelt efter sikkerhedsstandarden ISO27001.

Yderligere skal ministeriernes it-tilsyn med egne myndigheder styrkes. It-tilsynet med de statslige myndigheders informationssikkerhed er tilrettelagt som en del af det almindelige ministerielle tilsyn. It-tilsynet skal sikre, at myndighederne overholder centrale krav til informationssikkerhed, og at de ansvarlige myndigheder kan dokumentere, at de har den fornødne sikkerhed på deres områder.

På en række områder fører staten endvidere et særligt tilsyn med fokus på it-sikkerheden inden for deres område eller en sektor inden for eget ressort. Eksempelvis fører Erhvervs- og Vækstministeriet tilsyn med persondatasikkerheden i telesektoren, og Finanstilsynet fører tilsyn med it-sikkerheden i de finansielle virksomheder. De relevante myndigheder er omtalt i bilag 1.

Nøglen til at højne cyber- og informationssikkerheden er at arbejde systematisk og standardiseret med området. Derfor skal alle statslige myndigheder implementere den internationale sikkerhedsstandard ISO27001. For at sikre en prioritering af dette arbejde udarbejdes et koncept for it-tilsynet. Konceptet skal anvendes på tværs af staten i alle myndigheder medmindre særlige hensyn taler imod, fx fordi der hos en myndighed findes et andet, tilsvarende egnet tilsynskoncept. Derved understøttes ministerierne i at foretage en systematisk kontrol med egne myndigheders informationssikkerhed.

Ved at alle statslige myndigheder tager udgangspunkt i den samme informationssikkerhedsstandard og anvender det samme tilsynskoncept, sikres en øget professionalisering i form af et fælles sprog, fælles fremgangsmåder, fælles tiltag og en systematisk tværgående styring af indsatsen.

Ved at understøtte ministeriernes it-tilsyn fastholdes princippet om, at det er de enkelte myndigheder, der har ansvaret for at opbygge og udvikle en it-sikkerhedsorganisation samt at vurdere de relevante udfordringer og løsninger for den enkelte organisation.

2.2 Beskrivelse af indsats og initiativer

Kernen i indsatsen for at professionalisere det statslige arbejde med cyber- og informationssikkerhed er implementeringen af den internationale sikkerhedsstandard ISO27001 i de statslige myndigheder, samt ministeriernes it-tilsyn med egne myndigheder. Men dette arbejde kan ikke stå alene.

Myndigheder og virksomheder skal have adgang til relevant viden og de relevante kompetencer på cyber- og informationssikkerhedsområdet. Derfor styrkes arbejdet med videndeling om informationssikkerhedsarbejdet i den offentlige sektor. Derudover styrkes arbejdet med forskning og uddannelse inden for cyber- og informationssikkerhed, da det er centralt for det langsigtede arbejde med at styrke indsatsen på området.

Sikkerhedsstandarden ISO27001	**Sektoransvars-princippet**	**Statens Informationssikkerhedsforum**
ISO27001 er en international standard for informationssikkerhed. Standarden omfatter principper for risikovurdering, for ledelsens aktive stillingstagen hertil og for dokumentation af arbejdet med cyber- og informationssikkerhed. Med ISO27001 sker der således en tydelig ledelsesforankring heraf. De systematiske rutiner for risikoledelse og risikostyring, som er en del af standardens krav, understøtter en professionalisering af arbejdet i myndighederne.	Princippet indebærer, at den myndighed eller virksomhed, som til dagligt har ansvaret for et område, også har ansvaret for sikkerheden på området, herunder opretholdelsen af funktioner inden for ansvarsområdet ved en sikkerhedshændelse. Myndigheders ansvar for sikkerhed og beredskab i en sektor følger således af deres myndighedsansvar i øvrigt over for sektoren. Princippet anvendes generelt i det nationale beredskabsarbejde i Danmark.	Digitaliseringsstyrelsen har et forum for statslige myndigheder, Statens Informationssikkerhedsforum (SISF), som samarbejder om it-sikkerhedsområdet på et praktisk niveau. Det er myndighedernes informationssikkerhedskoordinatorer, der deltager i forummet. SISF fungerer i dag primært som videndelingsforum, men forummet er sammensat, så det fremover vil udgøre et velegnet forum til koordination af den praktiske håndtering af konkrete udfordringer.

Initiativer

1 Styrket arbejde med informationssikkerhed i staten

Der er behov for, at myndighederne professionaliserer deres tilgang til informationssikkerhed gennem en systematisk efterlevelse af den obligatoriske sikkerhedsstandard ISO27001, herunder også en mulig forenklet form for implementering af standarden. Det skal sikres, at informationer og systemer er beskyttet, herunder at myndighedernes risikostyring bliver professionaliseret. Myndighedernes arbejde skal tage udgangspunkt i opdaterede trusselsbilleder og viden om sårbarheder. Derudover er der behov for at understøtte arbejdet med it-tilsynet i staten via et fælles tilsynskoncept, der som udgangspunkt skal anvendes af alle ministerier, og som skal understøtte, at ministerierne løfter deres tilsynsforpligtelse. I overensstemmelse med sektoransvarsprincippet kan de enkelte ministerier anvende en anden form for tilsyn, hvis særlige hensyn taler herfor, og forudsat at tilsynet har samme høje niveau som det fællesstatslige. Der skal endvidere ske en opfølgning på ministeriernes arbejde med it-tilsynet. Derfor igangsætter Digitaliseringsstyrelsen følgende initiativer:

- Vejledning, herunder anvisning af modeller for en forenklet implementering af ISO27001 afhængig af organisatorisk størrelse og kompleksitet.
- Udarbejdelse af en handlingsplan for Digitaliseringsstyrelsens fremadrettede arbejde med vejledninger og værktøjer til implementeringen af ISO27001. Denne handlingsplan skal understøtte myndighedernes implementeringsplaner i forbindelse med overgangen til ISO27001. Handlingsplanen skal foreligge inden udgangen af 1. kvartal 2015. ISO27001 skal være implementeret af myndighederne primo 2016.
- En statusopfølgning på myndighedernes implementering af standarden foretages i juni 2015 i form af en spørgeskemaundersøgelse. Derudover vil der ske en opfølgning på den endelige implementering i andet kvartal 2016.
- Etablering af et virtuelt videnscenter for "Implementering af ISO27001 i staten" i samarbejde med Statens It.
- Udvikling af et statsligt tilsynskoncept, der kan understøtte ministeriernes it-tilsyn på eget ministerområde. Tilsynskonceptet vil give ministerierne konkrete anvisninger til deres egne interne tilsyn. Tilsynskonceptet skal være færdigudviklet medio 2015. Konceptet skal anvendes af alle ministerier, medmindre ministeriet kan dokumentere, at ministerområdet i forvejen følger et andet koncept for tilsyn målrettet deres særlige behov, og som er på samme niveau eller højere og kan argumentere for at bibeholde dette. Konceptet vil indeholde fastlæggelse af årshjul, tilsynsniveauer, organisering mv. for tilsynet. Derudover vil det indeholde fastlæggelse af særlige fokusområder for tilsynet, herunder; udvalgte tekniske sikkerhedsforanstaltninger, efterlevelse af ISO27001, sikring mod cybertrusler, systematiske risikovurderinger, leverandørkontrakter og opfølgningen på disse mv.
- En opfølgning på alle ministeriernes tilsyn gennemføres medio 2016.

2 Sikkerhedsmæssig risikovurdering i offentlige it-projekter

En professionalisering af sikkerheden i offentlige it-projekter kræver, at myndighederne bliver bedre til at foretage sikkerhedsmæssige risikovurderinger ved udbud eller indkøb af it-leverancer. Især er det vigtigt, at myndighederne gennemfører sikkerhedsmæssige risikovurderinger i analysefasen af større it-projekter. Desuden er det vigtigt, at myndighederne i offentlige it-projekter som grundlæggende præmis arbejder med privatlivsbeskyttelse, jf. overvejelserne bag "privacy-by-design". Derfor igangsætter Digitaliseringsstyrelsen følgende initiativer:

- I 2015 indarbejdes krav om en privatlivsrelateret og sikkerhedsmæssig risikovurdering i vejledningen til Statens It-projektmodel, der skal anvendes af alle it-projekter, og i den fællesstatslige programmodel, der skal anvendes for programmer over 60 mio. kr. med et væsentligt indhold af it.
- Kandidater med it-sikkerhedsfaglige kompetencer rekrutteres i 2015 til det fællesstatslige vurderingskorps, der bistår Statens It-projektråd med at gennemføre risikovurderinger af statens større it-projekter og -programmer.
- Statens It-projektråd øger i 2015 sit fokus på, at relevante sikkerhedsmæssige udfordringer håndteres, herunder at de fornødne sikkerhedsmæssige kompetencer er til stede hos myndighederne ved afvikling af de statslige it-projekter og -programmer.

3 Fællesoffentlig koordinering af informationssikkerhed

Der skal sikres en bedre fællesoffentlig koordinering, videndeling og hændelseshåndtering af informationssikkerhed på tværs af de offentlige parter (stat, kommune og region). Den øgede koordinering skal hjælpe den samlede offentlige sektor til en mere systematisk og ensartet tilgang til informationssikkerhed. Derfor vil Digitaliseringsstyrelsen:

- I 2015 etablere en fællesoffentlig koordination på ledelsesniveau for håndteringen af informationssikkerheden på tværs af den offentlige sektor.

4 Cyber- og informationssikkerhedsnetværk blandt uddannelses- og forskningsinstitutioner

Aktiviteterne på uddannelses- og forskningsområdet inden for cyber- og informationssikkerhed er i dag relativt fragmenterede, og der er for lidt viden om den uddannelse og forskning, der foregår på området. Derfor vil Uddannelses- og Forskningsministeriet primo 2015:

- Gennemføre en kortlægning af viden og uddannelsesaktiviteter på uddannelses- og forskningsinstitutionerne inden for cyber- og informationssikkerhed.
- Etablere et cyber- og informationssikkerhedsnetværk i samarbejde med de relevante videninstitutioner.

5 Styrket dialog mellem private og offentlige aftagere og de relevante uddannelses- og forskningsinstitutioner

Det er nødvendigt med en tættere kontakt mellem videninstitutionerne og private og offentlige aftagere om cyber- og informationssikkerhed. Denne skal styrke den gensidige forståelse af fremtidige behov og udfordringer og samtidig sikre et tættere samarbejde om udvikling og styrkelse af forskning og uddannelse på området. Det kan fx være at øge muligheden for, at forskere og studerende kan få adgang til relevante data og ressourcepersoner i forbindelse med uddannelsesforløb eller konkrete forskningsprojekter. Derfor vil Uddannelses- og Forskningsministeriet:

- Understøtte en tæt dialog mellem cyber- og informationssikkerhedsnetværket, jf. initiativ 4, og de centrale offentlige og private aftagere. Det skal sikre et øget samarbejde og en løbende og prioriteret afklaring af de fremadrettede behov for kompetencer og viden.

6 Kapacitet i Statens It til håndtering af cyberangreb

Statens It vil etablere et bedre grundlag for håndtering af cyberangreb mod Statens It's systemer og mod systemer, som Statens It leverer til tilsluttede myndigheder. Statens It vil herunder forstærke sit beredskab og forøge organisationens viden om cybersikkerhed. Dette skal sikre, at Statens It hurtigere opdager tegn på angreb og kan agere hurtigt på informationer fra Center for Cybersikkerhed eller leverandører om tegn på angreb. Samtidig vil Statens It hurtigere kunne iværksætte effektive sikringstiltag ved sikkerhedshændelser. Derfor vil Statens It:

- I 2015 opbygge øget kapacitet for håndtering af cyberangreb. Der udarbejdes en handlingsplan for området. Erfaringer fra gennemførelsen af handlingsplanen i Statens It kan efterfølgende udbredes til andre myndigheder med sigte på et løft i styring af andre leverandører i relation til sikkerhed.

3.0 Klare krav til leverandører

3.1 Målsætning for området

En stor del af den statslige digitale infrastruktur drives af eller i samarbejde med eksterne leverandører. Samarbejdet med professionelle aktører med stor viden inden for udvikling og drift af it-løsninger giver generelt gode muligheder for en stærk cyber- og informationssikkerhed. En central forudsætning er dog, at myndighederne som led i deres kontrakt- og leverandørstyring arbejder systematisk med cyber- og informationssikkerhedsområdet på linje med opfølgningen på andre dele af leverandørens performance.

En central del af arbejdet med cyber- og informationssikkerhed er derfor, at myndighederne stiller klare sikkerhedsmæssige krav til leverandørerne og løbende følger op på, at de overholdes. De statslige myndigheder skal arbejde mere systematisk med løbende at vurdere sikkerhedsniveauet i de løsninger, som drives af eksterne leverandører. Dette gælder også, hvor leverandøren er en anden offentlig myndighed som fx Statens It. Myndighedernes arbejde med den sikkerhedsmæssige leverandørstyring skal følge sikkerhedsstandarden ISO27001.

3.2 Beskrivelse af indsats og initiativer

I august 2014 udgav Center for Cybersikkerhed og Digitaliseringsstyrelsen rapporten "Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift". Rapporten indeholder en række anbefalinger til statslige myndigheder, som sigter på at styrke sikkerheden i statens outsourcede it-drift. Når myndigheder benytter eksterne leverandører til drift af digitale løsninger, skal der foreligge en klar aftale om håndteringen af it-sikkerheden i systemet. Den skal sikre et solidt grundlag for, at myndighederne kan stille krav til og foretage en løbende opfølgning på de eksterne leverandørers cyber- og informationssikkerhedsarbejde. Tilgangen skal være risikobaseret.

I rapporten "Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift" er hovedanbefalingerne:

1. At myndighederne går i dialog med leverandøren med henblik på at sikre, at alle leverandører gennemfører relevante tiltag for at opnå den ønskede sikkerhed i de leverede ydelser.
2. At myndighedernes risikovurdering og risikoledelse tager udgangspunkt i et opdateret trusselsbillede både ved nyudvikling, drift og videreudvikling af it-løsninger.
3. At ledelsen indgår i en aktiv dialog internt i myndigheden om efterlevelse af de øvrige anbefalinger i rapporten.

Det betyder, at myndighederne skal prioritere indsatsen efter behov og sikre en balanceret indsats, der vægter hensyn til brugervenlighed, sikkerhed og økonomi.

En professionel leverandørstyring er med til at sikre et højt offentligt informationssikkerhedsniveau. Sammen med en systematisk implementering af ISO27001 sikrer disse krav et stærkt og langtidsholdbart grundlag for et fortsat højt tillidsniveau til den offentlige digitale infrastruktur.

Målsætningen for indsatsen på området er at sikre, at der stilles relevante krav til og sker en løbende risikovurdering af og opfølgning på myndigheders eksterne leverandørers it-sikkerhedsarbejde.

Initiativer

7 Sikkerhedsmæssige krav i udbud og ved indgåelse af kontrakter på it-området

Der er behov for, at statslige myndigheder fremover arbejder mere systematisk med at inddrage sikkerhedsmæssige krav i forbindelse med udbud og ved indgåelse af kontrakter på it-området. Formålet er at øge kvaliteten af de sikkerhedsmæssige krav, der stilles til leverandører fremover. Derfor igangsætter Digitaliseringsstyrelsen følgende initiativer:

- En systematisk erfaringsudveksling af sikkerhedsmæssige krav mellem relevante myndigheder, der udbyder og indgår kontrakter på it-området. Arbejdet skal ske med tæt inddragelse af de relevante myndigheder og igangsættes i 2015.
- Støtte til myndighederne i forbindelse med indgåelse af it-kontrakter i form af en liste over sikkerhedsmæssige krav, som myndighederne kan bruge som inspiration i arbejdet med it-kontrakter. Dermed forenkles det at stille hensigtsmæssige sikkerhedskrav i it-kontrakter.
- En udarbejdelse af en ny standardkontrakt for it-driftskontrakter. Kontrakten skal bl.a. fokusere på at give myndighederne et godt udgangspunkt for at stille de rigtige sikkerhedsmæssige krav til leverandørerne ud fra en standardiseret ramme. Relevante myndigheder involveres i arbejdet.

8 Løbende opfølgning på den sikkerhedsmæssige leverandørstyring

Det er ikke nok, at myndighederne fastsætter passende sikkerhedsmæssige krav i kontrakter med eksterne leverandører. Der er også behov for, at myndighederne foretager en løbende opfølgning på, at kravene efterleves af leverandøren. Derfor vil Digitaliseringsstyrelsen:

- Følge op på de statslige myndigheders efterlevelse af og indarbejdelse af anbefalingerne i rapporten "Styrkelse af sikkerheden i statens outsourcede it-drift". Dette vil ske som en del af porteføljeoverblikket over it-driftskontrakter i regi af Rådgivningssekretariatet for it-drift, som udarbejder statusrapporter for statens outsourcede it-drift.

4.0 Styrket cybersikkerhed og mere viden på området

4.1 Målsætning for området

For at ledelsen i de statslige myndigheder og private virksomheder kan foretage en kvalificeret vurdering af risici på cyber- og informationssikkerhedsområdet, er det nødvendigt, at de kender til de aktuelle trusler mod deres systemer og data.

Den danske it-sikkerhedsbranche, som rådgiver om håndtering af trusler og sårbarheder i it-systemer og leverer sikkerhedsløsninger, bidrager til sikkerhedsarbejdet i hovedparten af alle offentlige myndigheder og private virksomheder.

Cyberangreb mod myndigheder og virksomheder inden for de sektorer, der beskæftiger sig med særligt samfundsvigtige funktioner, har dog potentielt så alvorlige konsekvenser for samfundet, at der er behov for, at der på cybersikkerhedsområdet suppleres med rådgivning, varsling og konkret håndtering fra statens side.

Med etableringen af Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste har regeringen sikret, at der i staten findes en myndighed med efterretningsbaseret viden om cybertrusler. Centret har som netsikkerhedstjeneste særlige muligheder for at understøtte myndigheders og virksomheders cybersikkerhed. Centret har således særlige forudsætninger for at varsle om konkrete trusler og bistå ved avancerede sikkerhedshændelser, der formodes at være et resultatet af angreb fra eller indtrængen via internettet.

Der er behov for at sikre, at myndigheder og virksomheder med funktioner af væsentlig betydning for samfundet som led i professionaliseringen af deres arbejde med cyber- og informationssikkerhed aktivt inddrager efterretningsbaseret viden om det aktuelle trusselbillede i deres risikovurderinger og sikkerhedsledelse. Herunder er der behov

Center for Cybersikkerhed

Som det statslige kompetencecenter for cybersikkerhed publicerer Center for Cybersikkerhed i dag varslinger og situationsbilleder om aktuelle trusler til de myndigheder og virksomheder, der er tilsluttet centerets netsikkerhedstjeneste. Netsikkerhedstjenesten har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder. Det sker med udgangspunkt i de af Center for Cybersikkerhed indhøstede erfaringer vedrørende avancerede trusler mod myndighederne og i informationer, som er modtaget fra centerets samarbejdspartnere. Desuden udgiver centeret situationsbilleder og trusselsvurderinger baseret bl.a. på information fra samarbejdspartnere og efterretninger.

for, at myndigheder og virksomheder i forsyningssektorerne har adgang til sektorspecifikke trusselsvurderinger og viden om trusler mod styringssystemer. Ligeledes er der behov for systematisk opsamling og behandling af erfaringer fra store sikkerhedshændelser i det offentlige.

Den offentlige sektor betjener sig i dag af mange internetforbindelser. Der er behov for en analyse af, hvordan den offentlige sektors forbindelser til internettet kan sikres, og hvordan det sikres, at statens myndigheder har tilstrækkelig mulighed for sikkert at udveksle følsom, herunder klassificeret, information.

Endelig er der behov for at styrke cyber- og informationssikkerheden i dansk erhvervsliv generelt, herunder i små og mellemstore virksomheder. Dette skal sikre, at myndigheder og især små og mellemstore virksomheder udnytter de eksisterende muligheder på sikkerhedsområdet fuldt ud.

4.2 Beskrivelse af indsats og initiativer

Der er allerede taget initiativer til at højne cybersikkerheden i staten, men implementeringen har ikke fundet sted på et tilstrækkeligt niveau. Regeringen har således i 2014 besluttet, at statslige myndigheder i deres it-miljøer skal implementere fire enkle, konkrete sikkerhedstiltag[1], og at myndighederne skal underrette Center for Cybersikkerhed ved større it-sikkerhedsmæssige hændelser. En fuld gennemførelse af disse beslutninger vil sammen med de klare krav til leverandører, som beskrevet i kapitel 3, give et væsentligt løft af cybersikkerheden i staten.

Regeringen vil sikre, at viden om cybertrusler i højere grad indgår i myndighedernes arbejde med cyber- og informationssikkerhed, så myndighederne har et tilstrækkeligt kendskab til de aktuelle trusler om cyberangreb. Til understøttelse heraf har Center for Cybersikkerhed indledt en systematisk dialog med ministerierne med deltagelse på afdelingschefniveau, med brancheorganisationer og med store virksomheder inden for de sektorer, der beskæftiger sig med samfundsvigtige funktioner. Der iværksættes herudover følgende initiativer til styrkelse af cybersikkerheden i Danmark:

[1] Tiltagene er beskrevet i vejledningen *Cyberforsvar der virker*, udgivet i december 2013 af Center for Cybersikkerhed sammen med Digitaliseringsstyrelsen.

Initiativer

9 Cybertrusler skal indgå i grundlaget for myndighedernes risikoledelse fra 2015

Regeringen vil sikre, at viden om cybertrusler i højere grad indgår i myndighedernes arbejde med cyber- og informationssikkerhed, så myndighederne har et tilstrækkeligt kendskab til de aktuelle trusler om cyberangreb. Center for Cybersikkerhed oplyser allerede om aktuelle trusler mod myndighedernes og sektorernes infra-struktur og data gennem varslinger og trusselbilleder. Der er dermed skabt et grundlag for, at cybertrusler kan indgå i myndighedernes risikoledelse. Derfor skal statslige myndigheder:

- Sikre, at cybertrusler indgår i myndighedernes risikovurderinger og risikoledelse fra 2015.

10 Etablering af enhed for vurdering af cybertrusler

Der etableres en enhed for vurdering af cybertrusler efter modellen for Center for Terroranalyse ved PET. Med udgangspunkt i udveksling af information om myndighedernes og sektorernes systemer og infrastruktur skal enheden udarbejde generelle og sektorspecifikke cybertrusselsvurderinger med henblik på at understøtte myndighedernes imødegåelse af cybertrusler på et så tidligt tidspunkt som muligt. Enheden skal bestå af en mindre fast stab og medarbejdere fra relevante myndigheder og sektorer. Derfor vil Center for Cybersikkerhed:

- Etablere en enhed for vurdering af cybertrusler under Center for Cybersikkerhed med deltagelse fra relevante sektorer med infrastruktur, som samfundsvigtige funktioner er afhængige af, samt andre relevante parter. Enheden etableres i første kvartal 2015 og opbygges gradvist i 2015-16.

11 Analyse af statens forbindelser til internettet

Regeringen ønsker en vurdering af modeller for, hvordan statens internetforbindelser kan samles og sikres, så staten som helhed alene anvender et begrænset antal sikrede internetforbindelser. Disse forbindelser skal, udover at anvende sædvanlige kommercielle sikkerhedsprodukter, være moniteret af Center for Cybersikkerheds alarmenheder med henblik på at opdage angreb og eventuelt filtrere kendt angrebstrafik. Derfor vil Center for Cybersikkerhed og Statens It:

- Tage initiativ til en analyse af, hvordan statens internetforbindelser kan samles og sikres. Analysen skal omfatte Access Points til understøttelse af sikker internetanvendelse fra mobile enheder. Analysens resultat skal foreligge inden udgangen af 2015.

12 Analyse vedrørende styrkelse af sikker kommunikation i staten

Regeringen ønsker en vurdering af, hvordan man kan styrke anvendelsen af infrastruktur til sikker udveksling af tjenstlig information mellem statslige myndigheder. Det ville i betydelig grad højne sikkerheden (fortroligheden) i kommunikation mellem myndigheder og bl.a. gøre det nemmere at dele klassificeret eller følsom information mellem myndighederne, fx oplysninger om cybertrusler fra Center for Cybersikkerhed. Et net til sikker intern kommunikation udgør ligeledes en meget lille angrebsflade for angreb fra internettet. Derfor vil Center for Cybersikkerhed med inddragelse af PET:

- Gennemføre en analyse vedrørende en styrkelse af sikker kommunikation i staten. Analysen vil fokusere på modeller for en udbredelse af det eksisterende REGNEM-net til statslige myndigheder. Analysens resultat skal foreligge inden udgangen af 2015.

13 Enhed til undersøgelse af større cybersikkerhedshændelser

Regeringen har indført, at alle statslige myndigheder skal underrette Center for Cybersikkerhed ved større cybersikkerhedshændelser. Blandt de cybersikkerhedshændelser, som indrapporteres, vil der være hændelser, som er særligt alvorlige. Regeringen ønsker, at der sker relevant udredning og analyse af sådanne hændelser. Samtidig skal det sikres, at erfaringerne fra hændelserne opsamles og i størst muligt omfang stilles til rådighed for andre myndigheder og virksomheder, således at erfaringerne kan anvendes aktivt i arbejdet med at forebygge fremtidige hændelser. Derfor vil Center for Cybersikkerhed:

- Etablere en enhed til undersøgelse af større cybersikkerhedshændelser. Enheden består som udgangspunkt af medarbejdere fra Center for Cybersikkerhed. Andre myndigheder – fx Digitaliseringsstyrelsen og PET – inkluderes afhængig af hændelsen. Enheden etableres i 1. kvartal 2015.

14 SCADA-kompetencecenter i Center for Cybersikkerhed

SCADA (indlejrede industrielle styringssystemer) anvendes bredt i forsyningssektorerne og i industrien. De udgør en sårbar angrebsflade for hackere, og der er ikke bredt tilgængelige sikkerhedskompetencer på området. Derfor vil Center for Cybersikkerhed:

- Etablere et særligt kompetencecenter på SCADA-området. Kompetencecenteret kan bistå og rådgive både private og offentlige virksomheder i forsyningssektorerne med viden om sårbarheder ved SCADA-systemer. Klima-, Energi og Bygningsministeriet inddrages i arbejdet. Kompetencecenteret etableres i 1. kvartal 2015.

15 Etablering af Virksomhedsråd for It-sikkerhed

Som led i "Vækstplan for digitalisering i Danmark" tages der initiativ til et virksomhedsråd, der gennem dialog og erfaringsudveksling skal understøtte en højnelse af it- og datasikkerheden i virksomheder og rådgive om, hvordan den digitale sikkerhed i dansk erhvervsliv kan styrkes. Derfor vil Erhvervs- og Vækstministeriet:

- Etablere et virksomhedsråd for it-sikkerhed, jf. vækstplanen.

5.0 Robust infrastruktur i energisektoren og telesektoren

5.1 Målsætning for området

Som et særligt indsatsområde har regeringen fokus på at styrke cyber- og informationssikkerheden i energisektoren og telesektoren. Området er udvalgt, fordi kravene til cyber- og informationssikkerhed for disse sektorer skal afspejle, at cyberangreb i disse sektorer kan have væsentlige samfundsforstyrrende konsekvenser.

Alvorlige energiafbrydelser, især strømafbrydelser, kan medføre en lang række alvorlige forstyrrelser af forskellige samfundsfunktioner. Dansk erhvervsliv og befolkning forventer en meget høj stabilitet i energiforsyningen i Danmark. Denne stabilitet skal bevares.

Tilsvarende er samfundsvigtige funktioner i alle sektorer dybt afhængige af et højt cyber- og informationssikkerhedsniveau i elektroniske kommunikationsnet og -tjenester, som udbydes af virksomhederne i telesektoren.

Vigtigheden af cyber- og informationssikkerhed på energi- og teleområderne er ikke ny, og danske virksomheder på disse områder har længe haft fokus på at opbygge en cyber- og informationssikkerhedsindsats.

For at styrke og fremskynde denne udvikling er der dog behov for på energiområdet, i første omgang i el- og naturgassektorerne, at foretage en gennemgang af virksomhedernes cyber- og informationssikkerhed og herudfra fastlægge nye krav til, hvordan virksomhederne kan øge deres indsats på området. Tilsvarende skal der på teleområdet fastsættes nye og skærpede regler for informationssikkerheden, der kan tage højde for de særlige problemstillinger, som er knyttet til teleudbydernes anvendelse af udenlandske leverandører.

Formålet med indsatsen i de to sektorer er således at fremtidssikre reguleringen heraf, så der fortsat kan være tillid til en høj driftsstabilitet og sikkerhed på områderne.

5.2 Beskrivelse af indsats og initiativer

El- og naturgassystemerne er i stort omfang automatiserede og afhængige af digitale styrings- og overvågningssystemer. Systemerne bliver i stigende omfang udbygget og integreret med andre systemer, og regeringen har fokus på, at det sker på en sikker måde. Udviklingen er en central forudsætning for den grønne omstilling på energiområdet.

Det forudsætter en løbende og fokuseret styring af både de mange involverede parter og den tekniske kompleksitet, som det er at opretholde cyber- og informationssikkerhed på energiområdet.

I telesektoren udlægger udbyderne i stigende grad driften og administrationen til underleverandører. Nogle lande har ud fra en risikobetragtning fundet anledning til helt at udelukke visse leverandører eller begrænse deres adgang til at levere udstyr og drift af infrastruktur, som anses for at have særlig betydning for samfundet. Regeringen finder, at hensynet til den nationale sikkerhed tilsiger, at der i forhold til teleudbydere fastsættes nye og skærpede regler for informationssikkerheden, der kan tage højde for de særlige problemstillinger, som er knyttet til teleudbydernes anvendelse af leverandører. Reglerne vil blive udformet, så de er så enkle som muligt og ikke pålægger teleudbyderne unødvendige administrative byrder.

Initiativer

16 **Styrkelse af net- og informationssikkerheden i samfundet**

Regeringen har, under hensyntagen til teleudbydernes rammer for investeringer, fokus på at sikre en styrket leverandørstyring på teleområdet og på, at teleudbyderne gennemfører passende sikkerhedsforanstaltninger overfor deres leverandører, så der ikke er svagheder i cyber- og informationssikkerheden i de kommunikationsnet og tjenester, som udbydes på det danske marked.

For at styrke net- og informationssikkerheden på teleområdet vil regeringen indføre ny regulering på området. Derfor vil forsvarsministeren:

- Fremsætte forslag til en ny lov om net- og informationssikkerhed i 2015.

17 **Opgradering af kravene til cyber- og informationssikkerhed på energiområdet**

Klima-, Energi- og Bygningsministeriet er i færd med at foretage en undersøgelse af niveauet for cyber- og informationssikkerhed i virksomhederne inden for el- og naturgassektorerne. Undersøgelsen er central for det fremadrettede arbejde med afdækning af risici og sårbarheder på området. På det grundlag udarbejdes forslag til tiltag til at sikre infrastrukturen. Heri vil indgå organisering, styring og regulering af virksomhederne, herunder sammenhængen med virksomhedernes beredskab.

På baggrund af undersøgelsen gennemfører Klima-, Energi- og Bygningsministeriet i løbet af 2015 og 2016:

- En undersøgelse primo 2015 af niveauet for cyber- og informationssikkerhed i virksomheder i el- og naturgassektorerne.
- Ændringer af elforsyningsloven og naturgasforsyningsloven og anden relevant energilovgivning i folketingssamlingen 2015-2016, så denne lovgivning understøtter de nævnte tiltag.
- På grundlag af lovændringerne gennemføres i 2016 en styrkelse af kravene til cyber- og informationssikkerhed på energiområdet, primært i el- og naturgassektorerne, som vurderes at være de mest kritiske. Disse tiltag omfatter øgede krav til virksomhedernes arbejde med cyber- og informationssikkerhed.

6.0 Danmark som stærk international medspiller

6.1 Målsætning for området

Cyber- og informationssikkerhed fylder stadig mere på den internationale dagsorden. Emnet berører efterhånden de fleste internationale institutioner og en række områder af betydning for dansk udenrigspolitik. Internationale spørgsmål om cyber- og informationssikkerhed omfatter sikkerhedspolitiske, folkeretlige og menneskeretlige aspekter.

Der er behov for at styrke internationalt samarbejde og international regulering på området. Danske holdninger afspejler ønsket om et frit, globalt internet, hvor offentlige myndigheder, virksomheder og borgere trygt kan udnytte internettets muligheder, og hvor Danmark og dets partnere beskytter sig mod cyberangreb.

Regeringen vil arbejde for at støtte international regulering i relevante internationale fora, hvor cybersikkerhed drøftes, herunder i EU, FN, OSCE, NORDEFCO og NATO. Endvidere er der behov for mere internationalt samarbejde om forskning og uddannelse inden for området. Det stiller større krav til Danmarks samlede indsats inden for cyber- og informationssikkerhedsdiplomati.

I EU-regi har man vedtaget den Digitale Dagsorden for Europa, der bl.a. i februar 2013 førte til, at EU-Kommissionen og EU's udenrigstjeneste udsendte en fælles strategi for cybersikkerhed. Strategien har som overordnet formål at sikre et åbent og sikkert cyberspace. Et væsentligt initiativ som led heri var fremsættelsen af direktivforslaget om Net- og Informationssikkerhed (NIS-direktivet). Strategien har derudover brede målsætninger, som omfatter cyberrelaterede emner i den fælles udenrigspolitik og fremme og beskyttelse af fundamentale rettigheder på internettet med fokus på bl.a. ytringsfrihed og adgang til information.

NIS-direktivforslaget forventes vedtaget i 2015. Overordnet set har direktivforslaget til formål at sikre et højt niveau for net- og informationssikkerhed i EU ved bl.a. at pålægge medlemsstaterne og en bred række markedsoperatører at gennemføre en række organisatoriske og sikkerhedsmæssige foranstaltninger. Dette forventes eksempelvis at medføre en forpligtelse for medlemsstaterne til at samarbejde med myndighederne i de andre medlemsstater, mens markedsoperatørerne bliver pålagt en række sikkerhedskrav samt en anmeldelsespligt ved sikkerhedshændelser.

I OSCE (Organisationen for Sikkerhed og Samarbejde i Europa) arbejdes med tillidsskabende foranstaltninger inden for cybersikkerhed, væsentligst i form af åbenhed om landenes cybersikkerhedspolitik, -programmer mv. Også i FN-regi har cyber- og informationssikkerhed været på dagsordenen siden 1998.

Danmark arbejder i NATO for, at alliancen bliver i stand til at beskytte sin egen infrastruktur og udgøre et effektivt forum for drøftelser og eventuelt fælles modsvar i tilfælde af cyberangreb på et alliancemedlem.

6.2 Beskrivelse af indsats og initiativer

Det er vigtigt, at Danmark sætter sit fingeraftryk på internationale diskussioner om cyber- og informationssikkerhed, bl.a. også ved at påvirke den fremtidige internationale regulering på området. På den baggrund iværksættes følgende initiativer.

Initiativer

18 Styrkelse af det danske cyberdiplomati

En aktiv dansk rolle på området forudsætter en opprioritering af cyberdiplomati. Derfor vil Udenrigsministeriet:

- Styrke koordinationen af Danmarks internationale indsats gennem udnævnelse af en cyberkoordinator.
- Øge dansk engagement og tilstedeværelse ved de væsentligste internationale møder på området og sikre, at danske holdninger er bedst muligt repræsenteret, når der udvikles nye standarder og internationale aftaler på området.
- Opbygge kompetencer og viden i netværket af danske ambassader og diplomatiske missioner med henblik på at yde bedst mulig støtte til danske myndigheders arbejde for danske synspunkter og interesser på området.

19 Fremme af Danmarks holdning i internationale samarbejder om cyber- og informationssikkerhed

Danmark arbejder for, at internettet ikke udvikler sig til en international konfliktzone. Derfor vil Udenrigsministeriet:

- I relevante internationale fora såsom EU, FN (herunder ITU), OSCE og NATO arbejde for generelt at styrke cyber- og informationssikkerheden på den ene side og sikre menneskerettigheder på internettet på den anden side.

20 Nordisk samarbejde om forskning og uddannelse i cyber- og informationssikkerhed

Uddannelse og forskning inden for cyber- og informationssikkerhed omfatter mange forskellige discipliner, hvor det inden for et meget specialiseret område kan være en udfordring at sikre en robust, kritisk masse og et stærkt fagligt miljø. Derfor vil det være hensigtsmæssigt at styrke samarbejdet mellem de nordiske lande om uddannelses- og forskningsindsatsen på området, også med henblik på at dele erfaringer om udviklingen på området. Der kan fx være basis for fælles forskningsprojekter, en særlig indsats i forbindelse med EU's forskningsprogram Horizon 2020 samt et øget uddannelsessamarbejde inden for cyber- og informationssikkerhed. Derfor vil Uddannelses- og Forskningsministeriet:

- I forbindelse med det kommende danske formandskab for Nordisk Ministerråd i 2015 tage initiativ til en dialog med de øvrige nordiske lande om mulighederne for at styrke samarbejdet om uddannelse og forskning på cyber- og informationssikkerhedsområdet.

7.0 Stærk efterforskning og klar information til borgere, virksomheder og myndigheder

7.1 Målsætning for området

I takt med digitaliseringen øges risikoen for it-kriminalitet, herunder hacking, cyberspionage og identitetstyveri. Derfor er det vigtigt, at Danmark er rustet til at kunne håndtere disse udfordringer, hvilket vil kræve en bred indsats. Borgere og virksomheder skal have den fornødne viden til at kunne tage vare på deres eget udstyr og egne data på nettet. Politiet skal have de fornødne kompetencer og ressourcer til at efterforske de nye kriminalitetsformer, og indsatsen for at håndtere kompromitteringer, når de først er sket, skal være effektiv og brugervenlig.

Borgere og virksomheder har et eget ansvar for egen adfærd og skal derfor støttes i at håndtere risikoen for it-kriminalitet på en fornuftig måde. Samtidigt er det vigtigt, at borgere og virksomheder kan få klar information og vejledning om, hvad de børe være opmærksomme på for at undgå at udsætte sig selv for unødige risici.

Det er centralt, at borgere og virksomheder oplever en enkel og effektiv behandling i de tilfælde, hvor de er blevet udsat for it-kriminalitet. For at understøtte dette skal politiet have de fornødne ressourcer og kompetencer til at efterforske de nye kriminalitetsformer.

7.2 Beskrivelse af indsats og initiativer

Borgere og virksomheder skal informeres om cyber- og informationssikkerhed og om mulighederne for selvstændigt at løse den sikkerhedsopgave, som følger af deres ansvar for beskyttelse af egne data og eget udstyr. Tilsvarende etableres et risikovurderingsbaseret sikkerhedstjek, som skal fremme virksomhedernes arbejde med cyber- og informationssikkerhed.

Parallelt med den præventive indsats styrkes politiets kompetencer og ressourcer i forhold til bekæmpelse af it-kriminalitet. Desuden styrkes indsatsen i forhold til at håndtere kompromitteringer, når de først er sket, med henblik på at ofre for it-kriminalitet oplever en effektiv og brugervenlig håndtering. Det forudsætter, at det nyligt etablerede Nationale Cyber Crime Center (NC3) fortsætter arbejdet med at opbygge et fagligt miljø, der er i stand til at følge med den hastige udvikling på området.

Initiativer

21 Højere sikkerhedsbevidsthed blandt borgere og virksomheder

Der er behov for at højne sikkerhedsbevidstheden blandt borgere og virksomheder i Danmark. Det indebærer blandt andet, at borgerne informeres bedre om sikkerheden i offentlige digitale løsninger og om nye sikkerhedsrisici, så borgerne er bedre rustet til at tage et selvstændigt ansvar for beskyttelsen af eget udstyr og egne data på nettet. Indsatsen foreslås tilrettelagt i samarbejde med relevante aktører i den private sektor, der vil bidrage til at øge borgernes og virksomhedernes bevidsthed om it-sikkerhed. Derfor vil Digitaliseringsstyrelsen:

- I løbet af 2015 gennemføre en informationsindsats målrettet borgere og virksomheder i Danmark. Indsatsens mål vil være at styrke kompetencerne blandt målgruppen, så de i højere grad kan tage ansvar for beskyttelse af data og udstyr. Digitaliseringsstyrelsen vil indgå et samarbejde med private parter og koordinere indsatsen med Erhvervs- og Vækstministeriet.
- Styrke informationsindsatsen på borger.dk med vejledning om it-sikkerhed og identitetstyveri mv.
- I samarbejde med Center for Cybersikkerhed, Undervisningsministeriet samt relevante offentlige og private parter tage initiativ til, at der laves en informationsindsats om cyber- og informationssikkerhed i folkeskolen.

22 Sikkerhedstjek for virksomheder

Regeringen tager som led i sin "Vækstplan for digitalisering i Danmark" initiativ til at fremme it-sikkerheden i dansk erhvervsliv. Der er behov for et større fokus på, om virksomhederne lever op til bestemte kriterier i forhold til informationssikkerhed. Derfor vil Erhvervsstyrelsen:

- Udvikle et risikobaseret it-sikkerhedstjek i samarbejde med relevante myndigheder som fx Center for Cybersikkerhed samt brancheorganisationer, som skal bistå virksomhederne med at leve op til centrale tekniske og informationsmæssige sikkerhedskrav. Tjekket skal bygge på eksisterende internationale standarder. Ordningen vil være frivillig, men Erhvervsstyrelsen vil gå i dialog med bl.a. revisorer, it-branchen og forsikringsbranchen med henblik på at fremme virksomhedernes brug heraf.

23 Udbygning af Nationalt Cyber Crime Center (NC3)

På baggrund af it-kriminalitetens eksplosive udvikling i de seneste år er Nationalt Cyber Crime Center (NC3) i 2014 etableret i Rigspolitiet. Med NC3 opbygges et stærkt fagligt miljø med specialistfunktioner og særligt avanceret teknologi til understøttelse af efterforskningen af it-kriminalitet. NC3 skal sammen med et kompetenceløft i politikredsene og et styrket strategisk og teknologisk fokus føre til en markant styrkelse og understøttelse af politiets og anklagemyndighedens behandling af straffesager om it-kriminalitet mv. NC3 skal bl.a. yde bistand til politikredsenes efterforskning af sager, som kræver særlig it-ekspertise, rutine eller udstyr. Herudover udarbejder NC3 i samarbejde med politikredsenes efterretnings- og analyseenheder analyser og efterforskningsoplæg til politikredsene.

NC3 har det overordnede ansvar for og tilsyn med politiets opgavevaretagelse vedrørende kriminalitet, der retter sig imod it-systemer, og kriminalitet, der begås under anvendelse af it, og hvor der afsættes digitale spor. Derfor vil NC3:

- Løbende vurdere udviklingsmulighederne på området og fortsætte arbejdet med at opbygge et fagligt miljø, der er i stand til at følge med den hastige udvikling på området.

24 Styrkelse af politiets rådgivning om informationssikkerhed

Politiets Efterretningstjeneste (PET) vil styrke sin rådgivningsindsats over for offentlige myndigheder og relevante virksomheder og organisationer, som håndterer klassificeret information og information af sikkerhedsmæssig betydning i øvrigt, og som kan være udsat for spionage og "insider-trusler".

Rådgivningen skal løfte informationssikkerheden ved bl.a. at sætte fokus på etablering af sikkerhedspolitikker og retningslinjer samt fysisk sikring af systemer og lokaliteter, hvor der opbevares og håndteres information af ovennævnte karakter.

Ligeledes skal rådgivningen også styrke informationssikkerheden gennem udvikling af sikkerhedskultur og ledelse, bl.a. ved øget fokus på rekrutteringsprocesser, medarbejderhåndtering, menneskelig adfærd og håndtering af menneskelige fejl. Derfor vil PET:

- I 2015 tilbyde undervisning og rådgivning til udvalgte myndigheder, virksomheder og organisationer om håndtering af trusler og risici relateret til informationssikkerhed.

25 Styrkelse af PET's kapacitet og kapabilitet på cyberområdet

PET's evne til at identificere, forebygge, imødegå og efterforske cybertrusler, der falder inden for straffelovens kapitel 12 (om forbrydelser mod statens selvstændighed og sikkerhed) og 13 (om forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme m.v.), herunder cyberspionage, cyberterrorisme og politisk motiverede cyberangreb, skal forbedres. Derfor vil PET:

- Styrke og udbygge PET's operative og strategiske analysekapacitet på cyberområdet.
- Sikre at den operative indsats understøttes gennem udvikling og tilgængelighed af de relevante it-redskaber.
- Gennemføre målrettet rekruttering og kompetenceudvikling af medarbejdere på cyberområdet.

Arbejdet indledes i 2015 og forventes i det væsentlige afsluttet i 2016.

26 Online anmeldelsesplatform

Når en borger eller virksomhed bliver offer for it-kriminalitet eller kriminalitet, der begås under anvendelse af it, har politiet særligt fokus på den forurettedes retssikkerhed og tryghed. Det sker gennem kompetent og effektiv reaktion samt ved rettidig og uangribelig bevissikring, så borgeren og/eller virksomheden beskyttes, og de ansvarlige kan drages til ansvar.

I den forbindelse skal det fremover være muligt at anmelde alle former for it-kriminalitet døgnet rundt, enten lokalt eller online via www.politi.dk. Dette skal blandt andet medføre, at NC3 kan sikre flygtige beviser, eventuelt i samarbejde med anmelder. Derfor vil Rigspolitiet:

- Styrke borgere og virksomheders mulighed for at anmelde it-kriminalitet mv. til politiet ved at udvikle en onlineplatform inden udgangen af 2015.

27 Blokering af stjålne identitetsoplysninger

For at mindske misbrug af stjålne eller bortkomne identitetsoplysninger kan der være behov for at etablere en "blokeringsordning" til politiets oplysninger om stjålne pas og kørekort, så offentligheden gives adgang til oplysninger om pasnummer og kørekortnummer for så vidt angår stjålne eller bortkomne pas og kørekort. Her-ved vil det være muligt for bl.a. teleselskaber, banker og andre finansieringsselskaber at validere, hvorvidt et kørekort- eller pasnummer er registreret som værende stjålet eller bortkommet. Derfor vil Rigspolitiet:

- Undersøge mulighederne og eventuelle hindringer ved etablering af en "blokeringsordning" til politiets oplysninger om stjålne pas og kørekort. Undersøgelsen forventes færdiggjort i 2015.

8.0 Opfølgning og det fremadrettede arbejde med cyber- og informationssikkerhed

Den teknologiske udvikling går stærkt, og arbejdet med cyber- og informationssikkerhed skal derfor løbende udvikles og udbygges. Med den nationale strategi er der sat en langsigtet fælles ramme for arbejdet.

En central del af arbejdet er, at myndighederne understøttes i at integrere et systematisk arbejde med cyber- og informationssikkerhed i deres almindelige virke. Ministerierne vil således selv skulle tilrettelægge den konkrete gennemførelse af initiativerne, fx i form af tidsplaner og fastlæggelse af milepæle. Sektoransvarsprincippet giver en klar ansvarsdeling og stærk forankring af initiativerne i strategien.

Afrapportering på strategien
Initiativerne skal være gennemført inden udgangen af 2016, med mindre særlige omstændigheder gør sig gældende. De enkelte ministerier er forpligtede til at forestå implementering og således også foretage en vurdering af, om særlige omstændigheder gør, at enkelte initiativer ikke kan gennemføres inden for tidsrammen.

Der gøres status for gennemførelse af strategiens initiativer første gang i maj 2015.

I oktober 2016 afrapporteres der om gennemførelsen af strategiens initiativer. I den forbindelse nedsættes en tværministeriel arbejdsgruppe. Arbejdsgruppen vil følge op på fremdriften i arbejdet med strategiens initiativer, herunder de tværgående initiativer, som skal implementeres bredt i staten, og forestå afrapporteringen.

Perspektivering
Som nævnt i afsnit 1.4 er det ikke muligt at opnå 100 pct. sikkerhed mod kompromitteringer, nedbrud mv. Informationssikkerhed er et anliggende, som berører hele samfundet. Det er derfor vigtigt, at alle tager ansvar for at højne sikkerheden. Det handler i høj grad om at skabe den nødvendige viden og kompetencer på området. Fx er det vigtigt, at børn tidligt lærer om god adfærd på internettet.

Regeringen sætter med denne strategi rammen for, at staten kan arbejde systematisk og professionelt med at fremtidssikre cyber- og informationssikkerheden i Danmark. I strategien er der en række tværgående initiativer, som vil betyde, at hele staten kan agere mere professionelt. Endvidere er der initiativer rettet mod energisektoren og telesektoren, fordi disse sektorer er helt centrale for de digitale systemer og andre samfundsvigtige funktioner, da energisektoren leverer energi (elektricitet), mens telesektoren udgør rygraden i samfundets kommunikation.

Med denne strategi iværksætter regeringen således en række væsentlige initiativer, men det er klart, at også andre sektorer og andre dele af den offentlige sektor (kommuner og regioner)

skal arbejde systematisk med cyber- og informationssikkerhed. Som nævnt i afsnit 1.5 vil der også blive sat fokus på kommunernes og regionernes arbejde med dette område i forbindelse med udarbejdelsen af den kommende digitaliseringsstrategi.

Endvidere er der igangsat en række andre aktiviteter, som har betydning for området. Blandt andet har Justitsministeriet nedsat en arbejdsgruppe, der skal vurdere beskyttelse af personoplysninger i forbindelse med elektroniske betalinger mv.

Derudover har regeringen i 2014 iværksat en række tiltag til at styrke cyber- og informationssikkerheden, som alle statslige myndigheder er forpligtet til at efterleve i 2014.

Cyber- og informationssikkerhed vil fortsat være et fokusområde for regeringen. I forbindelse med afrapporteringen på strategien kan effekten af ovennævnte aktiviteter indgå i en samlet vurdering af, hvor det vil være relevant at iværksætte nye initiativer. Ligeledes vil det blive vurderet, om der er behov for at inddrage andre sektorer fx finanssektoren i en opdatering af strategien. På baggrund af en vurdering af behovet for indsatser på nye områder samt en vurdering af de indhøstede erfaringer med denne strategi agter regeringen således i slutningen af 2016 at opdatere strategien for en ny periode.

Bilag 1

Myndigheder på området og en kort beskrivelse af deres opgaver

Beredskabsstyrelsen
Beredskabsstyrelsen forestår blandt andet den overordnede koordination af planlægningen af beredskabet i samfundet med henblik på at understøtte samfundets robusthed ved ulykker og katastrofer. Myndigheder og visse virksomheder inden for de enkelte sektorer indgår i beredskabet. Beredskabsstyrelsen udgiver årligt et nationalt risikobillede, som bør indgå i grundlaget for myndighedernes og virksomhedernes risikovurderinger.

Center for Cybersikkerhed
Center for Cybersikkerhed er etableret med udgangspunkt i regeringsgrundlagets målsætning om at samle statens kompetencer på cybersikkerhedsområdet i et center under Forsvarsministeriet. Center for Cybersikkerhed er som national it-sikkerhedsmyndighed, jf. Statsministeriets sikkerhedscirkulære, det nationale kompetencecenter på cybersikkerhedsområdet. Centret indeholder desuden Danmarks netsikkerhedstjeneste (GovCERT) og arbejder bredt med at understøtte en styrkelse af cybersikkerheden i den infrastruktur, som danner grundlag for samfundsvigtige funktioner.

Herunder er Center for Cybersikkerhed ansvarlig myndighed vedrørende informationssikkerhed, herunder cybersikkerhed, samt beredskab på teleområdet. Det indebærer, at centeret udarbejder reguleringen på området og varetager det løbende tilsyn med, at teleudbyderne efterlever reguleringens krav. Det er i henhold til teleloven teleudbydernes opgave at varetage informationssikkerheden i telenet og -tjenester. Udbyderne skal i den forbindelse planlægge et teleberedskab, for at samfundets beredskab i en beredskabssituation kan videreføre de væsentlige funktioner, som er afhængige af udbydernes net og tjenester. Teleloven og de dertil hørende bekendtgørelser om informationssikkerhed og beredskab implementerer EU's regler om informationssikkerhed og beredskab i den såkaldte teledirektivpakke.

Datatilsynet
Datatilsynet fører tilsyn med, at reglerne i persondataloven overholdes. Datatilsynet rådgiver og vejleder, behandler klager og gennemfører inspektioner hos myndigheder og virksomheder. Datatilsynet har også som opgave at føre tilsyn med behandling af personoplysninger.

DeIC (herunder DKCERT)
DeIC – Danish e-Infrastructure Cooperation – blev dannet i 2012 med det formål at understøtte Danmark som e-Science-nation gennem levering af e-Infrastruktur (computing, datalagring og netværk) til forskning og forskningsbaseret undervisning. DKCERT under DeIC følger sikkerheden på forskningsnettet og tilbyder en række ydelser på DeICs vegne til at forbedre sikkerheden. DeIC hører under Uddannelses- og Forskningsministeriet.

Digitaliseringsstyrelsen
Digitaliseringsstyrelsen blev dannet i 2011 af regeringen med det formål at stå i spidsen for omstillingen til et mere digitalt offentligt Danmark. På informationssikkerhedsområdet indtager styrelsen en koordinerende rolle med vejledninger til risikovurderinger og awareness. Styrelsen er også

OVERSIGT OVER MYNDIGHEDER PÅ CYBER- OG INFORMATIONSSIKKERHEDSOMRÅDET

CENTER FOR CYBERSIKKERHED

- Nationalt kompetencecenter på cybersikkerhedsområdet.
- National it-sikkerhedsmyndighed.
- Informationssikkerhedsmyndighed på teleområdet.
- Understøtter styrkelse af cybersikkerheden i den infrastruktur som samfundsvigtige funktioner er afhængig af.

DIGITALISERINGSSTYRELSEN

- Sikrer, at de statslige myndigheders informationssikkerhedsstyring lever op til de i staten obligatoriske principper.
- Rådgiver og vejleder statslige myndigheder om informationssikkerhed.
- Publicerer informationsmateriale rettet mod statslige myndigheder og borgerne for at øge bevidstheden om informationssikkerhed.

POLITIET

- Opklarer og efterforsker it-kriminalitet.
- Forebyggende indsats med henblik på at sikre, at it-kriminalitet ikke finder sted.
- It-sikkerhedsmyndighed på Justitsministeriets område.

DEN ENKELTE MYNDIGHED

- Ministerierne er ansvarlige for at føre it-tilsyn med egne myndigheder.
- Myndighederne er ansvarlige for egen informationssikkehed, herunder overholdelse af gældende regler for informationssikkerhed.
- Datatilsynet fører tilsyn med overholdelsen af reglerne i persondataloven.
- Rigsrevisionen fører tilsyn med statens myndigheder, herunder it-området.
- Statslige myndigheder fører sektortilsyn, fx Finanstilsynet.

ansvarlig for indførelsen af sikkerhedsstandarden ISO27001 i staten. Styrelsen fører tilsyn med Statens It på vegne af alle statens kunder.

Erhvervsstyrelsen
Erhvervsstyrelsen er ansvarlig for og fører tilsyn med persondatasikkerheden i telesektoren.

Finanstilsynet
Finanstilsynet fører tilsyn med it-sikkerheden i de finansielle virksomheder.

Nationalt Cyber Crime Center (NC3)
Rigspolitiet har pr. 1. maj 2014 etableret Nationalt Cyber Crime Center (NC3). Centret har bl.a. til opgave at efterforske og opklare it-kriminalitet, men har også et forebyggelseselement med henblik på at forhindre it-kriminalitet, fx krænkelse af børn på nettet.

Politiets efterretningstjeneste (PET)
PET er 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. PET er endvidere it-sikkerhedsmyndighed på Justitsministeriets område. PET arbejder således på at styrke overblikket over og reducere sårbarheder i de af Justitsministeriets systemer, der håndterer klassificeret information.

Udenrigsministeriet
Udenrigsministeriet arbejder for at styrke den samlede danske interessevaretagelse i internationale spørgsmål om cyber- og informationssikkerhed, herunder sikre, at danske holdninger er bedst muligt repræsenteret, når der udvikles nye standarder og internationale aftaler på området. Det vil ske gennem øget dansk engagement og tilstedeværelse i internationale fora, hvor cyber- og informationssikkerhed drøftes.

Bilag 2

Hvad er informationssikkerhed og cybersikkerhed

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.

- **Adfærd**
  Ledelsens og organisationens adfærd er af betydning for sikkerheden. God adfærd forudsætter, at ledelse og medarbejdere kender til hvilke data og systemer i organisationen, som er særligt beskyttelsesværdige. De skal kende til de eventuelle risici for kompromittering og kende til organisationens sikkerhedspolitik og foranstaltninger.

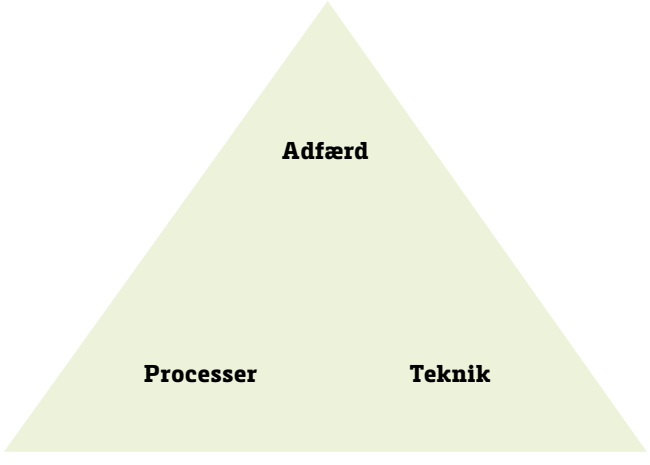
- **Processer**
  Organisationen skal have processer for løbende vurdering og opretholdelse af sikkerheden samt beredskaber i tilfælde af sikkerhedsbrud.

- **Teknik**
  Organisationen skal sørge for en fornøden teknisk sikring af data og systemer.

Det er ledelsens ansvar, at der løbende foretages en vurdering af risici og træffes beslutning om passende tiltag til opretholdelse af informationssikkerheden på de tre områder.

Alle tre elementer er nødvendige, og ingen af dem kan stå alene. En simpel analogi er sikringen af et hjem. Vi sætter lås på hoveddøren, men vi ved også, hvordan vi bruger en nøgle, og hvornår vi skal låse døren. Vi forstår formålet med låsen, så vi ikke forlader hjemmet med et åbent vindue eller overlader nøglen til en fremmed. Vi har en proces for at forlade hjemmet, idet vi kontrollerer for åbne vinduer, ser efter nøglen i lommen eller tasken, inden låsen slås til, og tager i døren for kontrollere, at den faktisk er låst.

ELEMENTER I INFORMATIONSSIKKERHED



Hver gang der sker ændringer i de forretningsmæssige mål i organisationen, i den tekniske platform eller i trusselbilledet, skal sikkerheden revurderes: Organisationens opgaver kan fx blive ændret, så den skal kunne håndtere nogle nye forretningsgange, der omfatter behandling af værdifulde eller følsomme data, som organisationen ikke tidligere var i kontakt med. Fx kan organisationen indføre et nyt system, som kræver uddannelse af brugerne, eller der kan ske salg af en kritisk leverandør til en ny ejer, som ikke agter at overholde kontraktens forpligtelser.

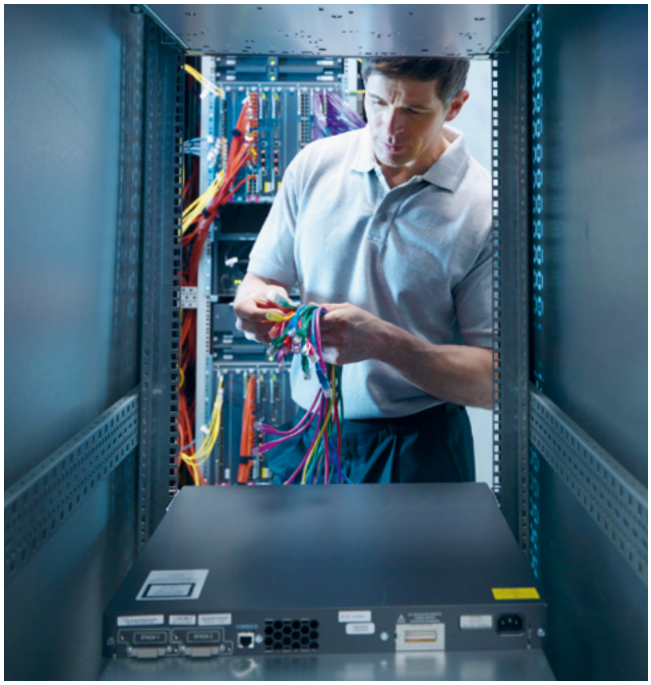
Det er udgangspunktet i ISO27001, som er den internationalt anerkendte standard for informationssikkerhed, og som er obligatorisk at anvende i staten, at styringen af informationssikkerhed sker ved inddragelse af den forretningsansvarlige ledelse, at den sker i et dokumenteret system, og at den sker på baggrund af en risikovurdering. Ledelsen er ansvarlig for, at der er indført passende sikring af de forretningsmæssige værdier, som ligger i organisationens data og systemer, i forhold til de risici, der måtte være for nedbrud, angreb udefra, leverandørsvigt mv.

Den konkrete risikovurdering skal i relevant omfang indeholde en vurdering af konsekvensen af et sikkerhedsbrud i et system. De fleste organisationer behandler i et vist omfang følsomme eller værdifulde data (såsom oplysninger af væsentlig økonomisk betydning for en virksomhed, oplysninger om forskeres originale ideer og forskningsresultater, oplysninger af betydning for statens sikkerhed eller rigets forsvar, personoplysninger mv.). Nogle organisationer driver systemer, hvis opretholdelse er af væsentlig betydning for samfundet. Under alle omstændigheder skal der med udgangspunkt i en konkret risikovurdering ske den relevante sikring.

Cybersikkerhed

Cybersikkerhed er den disciplin inden for informationssikkerhed, som omhandler sikkerheden ved tilgang til systemer udefra, herunder systemernes forbindelse mod internettet eller mod andre net og systemer, som er forbundet til internettet. En forbindelse til et andet system eller til internettet medfører, at et system er udsat for en række nye udefrakommende trusler. Afhængig af værdien af data og systemer og risici ved kompromittering skal der derfor foretages en række informationssikkerhedstiltag til imødegåelse af cybertrusler.

Blandt de mest grundlæggende tiltag er fx firewalls og antivirus, procedurer for medarbejderes brug af cloud-tjenester til organisationens data samt uddannelse af medarbejderne om risici ved brug af ukrypteret e-post, om risici vedrørende phishingforsøg og malware i indkommende mails, og om risici ved udveksling af data med USB-lagerenheder.



Relevante tiltag skal gennemføres som led i organisationens arbejde med informationssikkerheden. Da truslerne fra internettet kan være særligt teknisk avancerede, kræver det særlige forholdsregler og opbygningen af en særlig adfærd og særlig viden i organisationen.

Arbejdet med cybersikkerhed forudsætter, at organisationen løbende orienterer sig i de tilgængelige trusselsvurderinger, herunder de efterretningsbaserede varslinger og trusselsvurderinger fra Center for Cybersikkerhed, da trusler mod cybersikkerheden kan ændres meget hurtigt ved teknologiskift eller ved ændringer i angriberes kapaciteter og interesse.

Arbejdet med cybersikkerhed må tage udgangspunkt i, at angribere fra tid til anden kommer ind i systemerne. Scanning for malware, løbende opdatering af programmer og systemer og begrænsning af brugeres systemrettigheder til, hvad der opfylder det konkrete arbejdsmæssige behov for den pågældende, er enkle tiltag, som giver en angriber svære betingelser. Blandt mere avancerede tiltag er en intelligent overvågning af egne systemer. Tiltag såsom logning og monitering af afvigelse fra normalbilledet (trafik til og fra IP-numre, som man ikke ville forvente, usædvanligt store dataoverførsler) skal overvejes. En angriber anvender typisk en legitim brugers konto, så tiltag til at identificere usædvanlig brugeradfærd (logins fra andre punkter end normalt eller logins på usædvanlige tidspunkter) kan være mulige passende sikkerhedsforanstaltninger.

Bilag 3
Initiativoversigt

National strategi for cyber- og informationssikkerhed

Øget professionalisering og mere viden

2014/2015 : 09

Henvendelse om udgivelsen kan i øvrigt ske til
Forsvarsministeriet
Holmens Kanal 42
1060 København K
Tlf.: 72 81 00 00
E-mail: fmn@fmn.dk

ISBN
978-87-93214-47-7

Elektronisk publikation
978-87-93214-48-4

Design
e-Types & e-Types Daily

Foto
Polfoto
iStock

Tryk
Rosendahls Schultz Grafisk a/s

Web
Publikationen kan hentes på
fmn.dk

NORDISK MILJØMÆRKNING
541 016
Trykkeri