Energi-,
Forsynings- og
Klimaministeriet

# Cyber- og informations-sikkerhedsstrategi for energisektorerne

Cyber- og informationssikkerhedsstrategi for energisektorerne

# Resumé

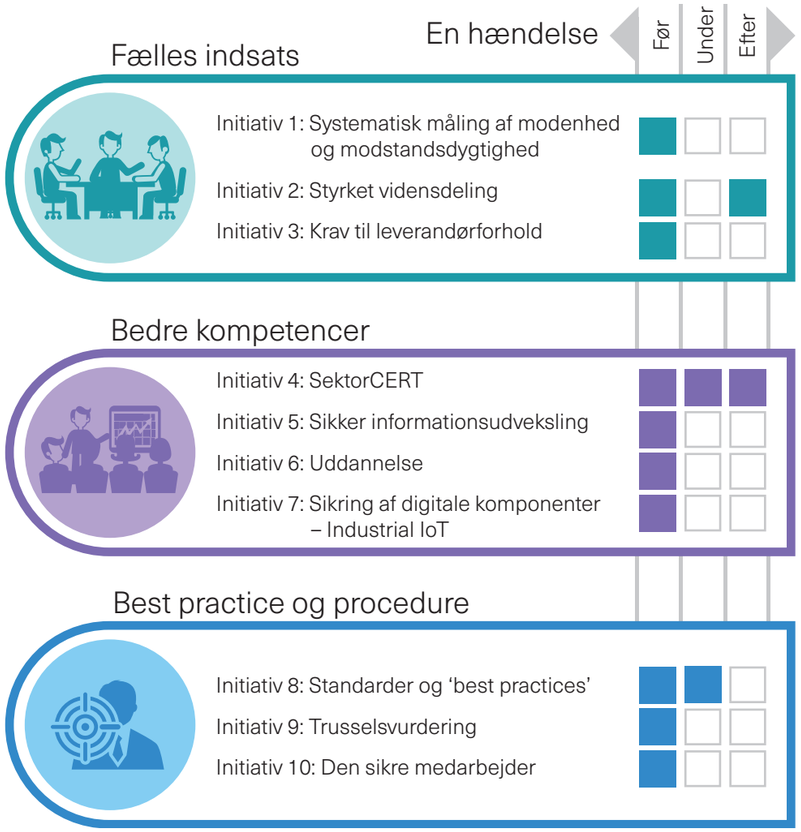
Der ses et forhøjet trusselsbillede for cyberangreb i energisektorerne i takt med den øgede digitalisering

Cyber- og informationssikkerhedsstrategien for energisektorerne (el, gas og varme) er udarbejdet af Energi-, Forsynings- og Klimaministeriet i samarbejde med interessenter fra de danske energisektorer heriblandt Dansk Energi, Energinet, Dansk Fjernvarme, Dinel, Radius og HOFOR. Strategien er en sektorspecifik forlængelse af regeringens nationale strategi for cyber- og informationssikkerhed 2018-2021, som blev lanceret i maj 2018 [1]. Det fremgår heraf, under initiativ 3.1, at der skal udarbejdes en cyber- og informationssikkerhedsstrategi for energisektorerne.

På baggrund af Center for Cybersikkerheds aktuelle trusselvurdering og Energinets risiko- og sårbarhedsvurderinger for energisektorerne er vurderingen, at der ses et forhøjet trusselsbillede [2] for cyberangreb i energisektorerne i takt med den øgede digitalisering i sektorerne og samfundet generelt, og at et angreb mod de danske energisektorer kan have alvorlige konsekvenser. Konsekvensen af et eventuelt angreb vil have forskellige konsekvenser afhængig af, hvilken sektor der rammes. Strategiens 10 konkrete initiativer skal styrke cyber- og informationssikkerheden i energisektorerne, så indsatsen følger den teknologiske udvikling, fremmer en fortsat kommerciel vækst og samtidig sikrer en stabil energiforsyning i en digitaliseret verden.

## Strategiens 10 konkrete initiative skal styrke cyber- og informationssikkerheden i energisektorerne

De 10 konkrete initiativer bygger ovenpå det store arbejde, der allerede er gjort for at sikre en høj cyber- og informationssikkerhed i sektorene. Initiativerne er fordelt i tre hovedemner. Denne tematiske gruppering har taget udgangspunkt i hovedemnerne i den nationale strategi 'fælles indsats' og 'bedre kompetencer', hvortil der er tilføjet emnet 'best practices og procedurer'. Initiativerne er derudover grupperet efter de overordnede arbejdsområder i et cyberangrebs hændelsesforløb – jf. figur 1.




*Figur 1: Initiativerne, hovedemner og arbejdsområder*

Cyber- og informationssikkerhedsstrategien for energisektorerne skal udmøntes i en sammenhængende og konkret programplan for det videre arbejde med initiativerne. Der skal leveres beslutningsgrundlag, rapporter og anbefalinger for at sikre en effektiv gennemførelse af initiativerne, som tilsammen forventes at kunne styrke arbejdet med cyber- og informationssikkerhed i energisektorerne i samarbejde med sektorerne.



# Indhold


# 1. Forord

Strategien indeholder en beskrivelse af baggrunden og behovet for en sektorspecifik strategi, en indledende risiko- og sårbarhedsvurdering af energisektorerne og en beskrivelse af behovet for et samarbejde på tværs af kritiske sektorer.



Energisektorernes sårbarhed over for cybertrusler udvikler sig hastigt i takt med digitalisering

En sikker energiforsyning er en forudsætning for et velfungerende samfund, og manglende sikkerhed i energisektorerne er dermed en sårbarhed for hele samfundet. På mine besøg ude i landet ser jeg, hvor hårdt varmeværker, elselskaber, forsyningsbranchen og industrien arbejder på at sikre en grøn og stabil energisektor i Danmark, og jeg ser også, hvor vigtig IT er på den rejse.

Energisektorernes sårbarhed over for 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 nabolandene og balanceringen af fluktuerende energiproduktion fra sol- og vindenergi.

Denne cyber- og informationssikkerhedsstrategi for energisektorerne er udarbejdet af Energi-, Forsynings- og Klimaministeriet i samarbejde med interessenter fra de danske energisektorer. Strategien er en sektorspecifik forlængelse af regeringens nationale strategi for cyber- og informationssikkerhed 2018-2021, som blev lanceret i maj 2018 [1].

Energi var også et fokusområde i den forrige nationale strategi for cyber- og informationssikkerhed 2015-2016 [3], hvor initiativerne for energisektoren mundede ud i udarbejdelsen af en bekendtgørelse om IT-beredskab for el- og naturgassektorerne. Denne bekendtgørelse udgør et fundament for denne nye strategis yderligere styrkelse af cyber- og informationssikkerheden i energisektorerne, som gennem 10 konkrete initiativer adresserer de forhold, der er identificeret i de forgangne års arbejde inden for området.

Strategien indeholder en beskrivelse af baggrunden og behovet for en sektorspecifik strategi, en indledende risiko- og sårbarhedsvurdering af energisektorerne og en beskrivelse af behovet for et samarbejde på tværs af kritiske sektorer i Danmark. Disse omhandler foruden energisektoren: sundhed, transport, tele, finans og søfart. Vi har brug for digitaliseringen, men vi skal ikke være blinde for udfordringerne, som kan komme med den. Derfor er jeg rigtig glad for det store arbejde, som er lagt i den nye strategi, og jeg håber, den kan skabe rammerne for, at vores grønne og stabile energisystem bliver endnu mere sikkert.

Lars Chr. Lilleholt
Energi-, forsynings- og klimaminister

# 2. Introduktion

### Øget digitalisering skaber nye udfordringer

Energisektorerne digitaliseres i disse år i Danmark såvel som internationalt. Digitaliseringen er en del af den teknologiske udvikling og er med til at fremme en fortsat kommerciel udvikling, hvor Danmark ønsker at være blandt verdens førende inden for integration af vedvarende energikilder, fremme et fleksibelt forbrug og sikre en høj forsyningssikkerhed.

Digitaliseringen medfører øget brug af computersystemer eller computerrelaterede enheder til systemer, der kommunikerer med eller er en del af det forsyningskritiske netværk i energisektorerne. Ved øget brug af digitalisering i energisektorerne øges digitale sårbarheder, hvilket kan medføre udfordringer for energisektorerne og den stabile energiforsyning i Danmark. Som følge af cyberangrebene i Ukraine i 2015 [4] og 2016 [5] var et større antal kunder i begge tilfælde uden strøm i en længere periode. Angrebene i Ukraine er eksempler på, hvordan digitale sårbarheder kan medføre direkte konsekvenser for forsyningen af energi. I 2017 var der cyberangreb mod den danske energisektor [6]. Disse angreb havde dog ikke konsekvenser for forsyningssikkerheden.

Danmark ønsker at være blandt verdens førende inden for integration af vedvarende energikilder, fremme et fleksibelt forbrug og sikre en høj forsyningssikkerhed



## Boks 1:

## Definition af informations- og cybersikkerhed

Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger, der sikrer informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. Inden for informationssikkerhed arbejdes der blandt andet med organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger.

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.

### Behov for en ambitiøs strategi for energisektorerne

En ambitiøs cyber- og informationssikkerhedsstrategi for energisektorerne skal yderligere styrke cybersikkerheden i de kritiske systemer og netværk inden for energisektorerne (el, naturgas og fjernvarme). Cyber- og informationssikkerhed er områder, der er i hastig udvikling, blandt andet som følge af trusselsaktørernes stadigt hyppige og avancerede angrebstyper.

Strategien er udarbejdet i samarbejde med sektorerne og indeholder 10 initiativer, der tilsammen skal styrke cybersikkerheden i energisektorerne yderligere. Strategien bygger oven på det store arbejde, der allerede er gjort i energisektorerne som følge af den nationale strategi for cyber- og informationssikkerhed 2015-2016 [3]. Tiltagene skal blandt andet minimere mulige cybersikkerhedshændelser og konsekvensen af disse mod den danske energisektor ved at være forberedt, når en hændelse sker, effektivt at kunne håndtere et hændelsesforløb og opnå viden om, hvordan kritiske systemer og netværk reetableres.

## Boks 2: Strategiens initiativer

| Fælles indsats | Bedre kompetencer | Best practices og procedurer |
|---|---|---|
| **Initiativ 1**: Systematisk måling af modenhed og modstandsdygtighed | **Initiativ 4**: SektorCERT | **Initiativ 8**: Standarder og best practices |
| **Initiativ 2**: Styrket vidensdeling | **Initiativ 5**: Sikker informationsudveksling | **Initiativ 9**: Trusselsvurdering |
| **Initiativ 3**: Krav til leverandørforhold | **Initiativ 6**: Uddannelse | **Initiativ 10**: Den sikre medarbejder |
| | **Initiativ 7**: Sikring af digitale komponenter - Industrial IoT | |

For at sikre et mere hensigtsmæssigt opgavesnit mellem Energistyrelsen og Energinet forventes det, at tilsynet bliver flyttet til Energistyrelsen pr. 1. juli 2019.

### Videre proces med strategien

Den nationale strategi for cyber- og informationssikkerhed er baseret på et fælles ansvar gennem effektivt samarbejde mellem sektorernes virksomheder og myndighederne. Energisektorerne har været involveret i udarbejdelsen af cyber- og informationssikkerhedsstrategien for energisektorerne gennem deltagelse i projektets styre- og arbejdsgruppe. I bilag A beskrives metoden bag udviklingen af strategien.

De konkrete initiativer i cyber- og informationssikkerhedsstrategien for energisektorerne skal efterfølgende udmøntes i et sammenhængende og konkret cyber- og informationssikkerhedsprogram, der dækker strategiperioden 2018-2021, og som skal koordinere det videre arbejde med initiativerne. Der skal leveres beslutningsgrundlag, rapporter og anbefalinger, som tilsammen forventes at kunne styrke arbejdet med cyber- og informationssikkerhed i energisektorerne.



# 3. Risiko- og Sårbarheds-vurdering for energisektorerne

Som et led i udarbejdelsen af cyber- og informationssikkerhedsstrategien er der lavet en kort og indledende risiko- og sårbarhedsvurdering (ROS-vurdering) af energisektorerne.

### Cyberangreb kan true forsyningssikkerheden af energi

Digitaliseringen i de danske energisektorer medfører en øget integrering af systemer og brug af offentlige forbindelser, som fx internettet. Digitalisering og brug af offentlige forbindelser øger risikoen for cyberangreb mod de kritiske energisystemer, da systemerne bliver mere tilgængelige, end de har været tidligere. Et cyberangreb mod de samfundskritiske energisystemer kan have konsekvenser, som er svære at vurdere omfanget af på forhånd. Et cyberangreb vil kunne true forsyningssikkerheden i den danske energiforsyning.

Et cyberangreb mod de samfundskritiske energisystemer kan have konsekvenser, som er svære at vurdere omfanget af på forhånd



Der er i de seneste år set destruktive angreb på energisektorerne i udlandet

El- og naturgassektorerne har arbejdet systematisk med at styrke cyber- og informationssikkerheden, især siden arbejdet med og ikrafttrædelsen af bekendtgørelsen om IT-beredskab i el- og naturgassektorerne i juli 2017. Heri stilles blandt andet krav til virksomhederne i el- og naturgassektorerne om periodisk udarbejdelse af en vurdering af relevante risici- og sårbarheder, der kan påvirke virksomhedens forsyningskritiske IT-systemer, samt beredskabsplanlægning baseret på den gennemførte ROS-vurdering.

### Aktuel trusselvurdering

Af Center for Cybersikkerheds (CFCS) trusselvurdering for energisektoren fra september 2018 [7] fremgår, at truslen fra cyberspionage og cyberkriminalitet er meget høj, hvor truslen fra cyberaktivisme og cyberterror er lav. Det vurderes også, at et destruktivt angreb fra fremmede stater mod energisektoren på kort sigt er mindre sandsynligt. Det vurderes samtidig, at denne sandsynlighed hurtigt kan ændre sig ved fx politiske eller militære konflikter. Der er i de seneste år set flere destruktive angreb på energisektorerne i udlandet [4, 9,10].

Destruktive angreb ændrer præmissen for arbejdet med cyber- og informationssikkerhed i de danske energisektorer. Med det aktuelle trusselsbillede vurderes det, at der er sandsynlighed for, at sårbarhederne kan udnyttes af aktører med fjendtlige intentioner.

### ROS-vurdering

CFCS' trusselsvurdering suppleres af ROS-vurderinger for energisektorerne udarbejdet af Energinet. Den første ROS-vurdering blev udarbejdet i 2017 og viste, at ROS-vurderinger er et effektivt værktøj, som forventes at have en væsentlig betydning for cyber- og informationssikkerheden i sektorerne.

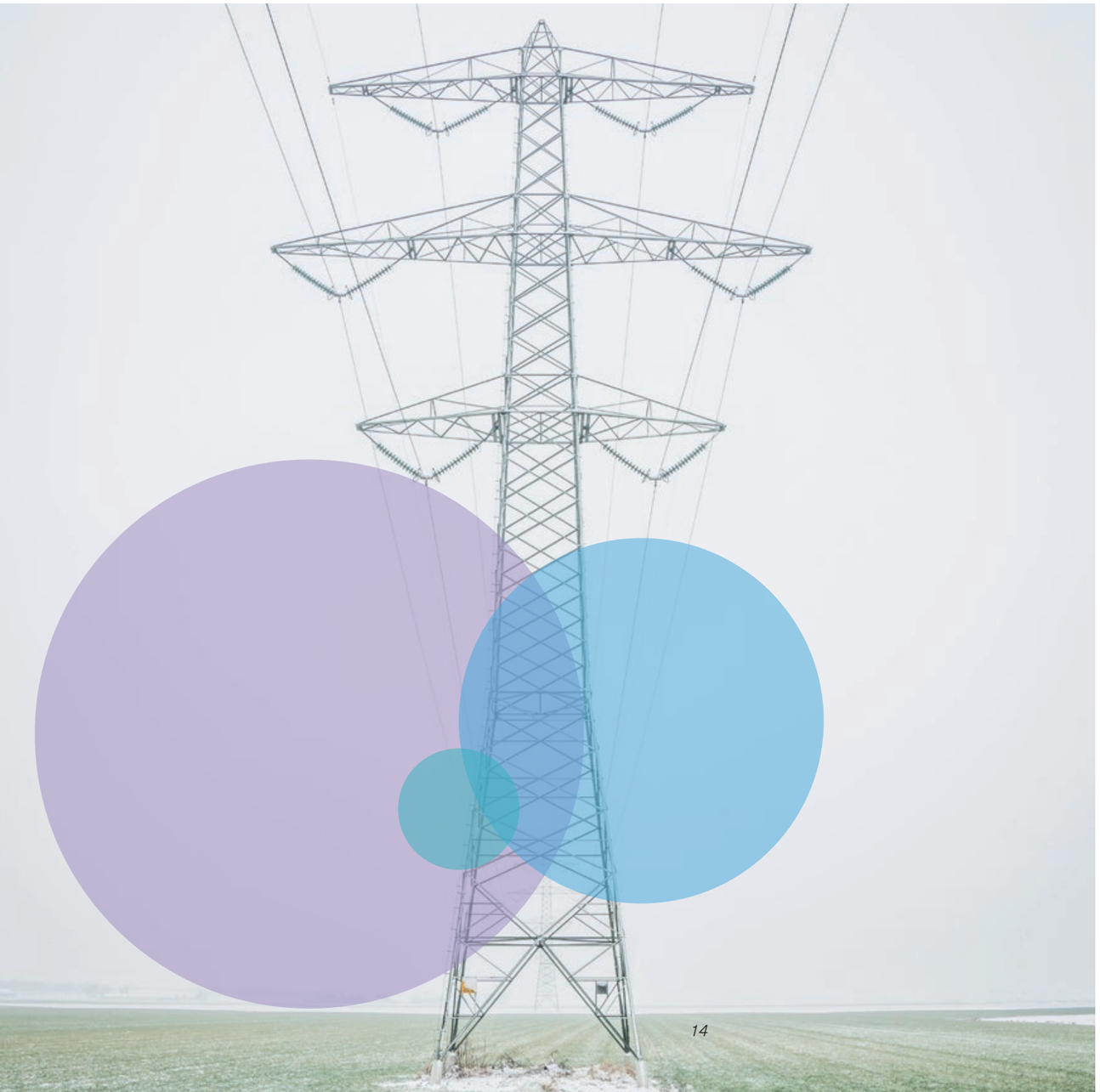
ROS-vurderingen for 2017 viste, at de største sårbarheder findes i forhold til virksomhedernes styringssystemer til energisystemerne. Her vurderede en overvejende del af virksomhederne, at angreb på disse vil have alvorlige konsekvenser for forsyningssikkerheden. Det skal understreges, at der er forskel på de styrings- og kontrolsystemer, der anvendes i sektorerne, hvilket vil vanskeliggøre et koordineret cyberangreb på tværs af virksomhederne. Energinet vurderede i øvrigt eksterne leverandører som en medvirkende faktor i forhold til sårbarheder.

ROS-vurderingen for 2018 er under udarbejdelse. I denne har virksomhederne skullet vurdere nogle nye scenarier i forhold til 2017-vurderingen. De nye scenarier er blandt andet udviklet på baggrund af erfaringerne med internationale cyberangreb i slutningen af 2017 [10]. Ifølge Energinet viser ROS-vurderingen for 2018 samme typer af sårbarheder som 2017-vurderingen. Virksomhederne er opmærksomme på sårbarhederne og arbejder med at beskytte systemerne via fx segmentering og funktionsadskillelse. I ROS-vurderingerne indgår ikke

en vurdering af sandsynligheden for cyberangreb, men det kan ikke udelukkes, at sandsynligheden øges som følge af en mere aktiv trussel.

**Sektorernes styringssystemer**

Styringssystemerne, som bruges i sektorerne, er komplicerede og består af mange elementer. Disse udskiftes sjældnere end andre almindelige IT-systemer. Udbedring af sårbarhederne via opdateringer er derfor ikke altid mulig, da opretholdelse af systemernes funktionalitet ikke kan garanteres. Styringssystemerne udgør derfor en sårbarhed over for den hastige udvikling i trusselsbillede.





To typer af cyberangreb vurderes at være mest sandsynlige; koordinerede angreb med specifikt formål og bredspektrede angreb

**Mest sandsynlige angrebsmetoder**

To typer af cyberangreb vurderes at være mest sandsynlige på baggrund af kendte angrebsmetoder[4,6,7,8,9,10,11]; koordinerede angreb med et specifikt formål og bredspektrede angreb, hvor sektorerne ikke nødvendigvis er det direkte mål. Det koordinerede angreb defineres som et APT-angreb (Advanced Persistent Threat), der har et specifikt formål og ofte er politisk motiveret. APT-angreb kan være svære at opdage, fx angrebet på energiforsyningen i Ukraine i 2015 [4] og 2016 [5]. Det bredspektrede angreb er ofte et angreb med et fjendtligt formål, der ikke nødvendigvis er målrettet energisektorerne, men kan have konsekvenser for energiforsyningen, fx et ransomware-angreb, der rammer de kritiske systemer.

Phishing- og supply-chain-angreb vurderes også at være sandsynlige angreb mod energisektorerne. Ved et phishing-angreb opnår angriberen adgang til fx et forsyningskritisk netværk via inficering af medarbejderes enheder. Det mest normale phising-angreb finder sted via en email med malware, som kan give fjernadgang til angriberen, uden at brugeren opdager dette. Et supply-chain-angreb er defineret ved, at angriberen på forhånd har inficeret en leverandørs enhed, og leverandøren inficerer derved de kritiske systemer ved at arbejde med fx sin PC på det kritiske netværk.

### Boks 3: Definition af malware

Malware (skadelig software) er et ondsindet program eller en del af et program. Det bruges som en fællesbetegnelse for en række kategorier af computerprogrammer, der foretager skadelige eller uønskede aktiviteter på de computere, de kører på.

**Konklusion og vurdering**

Konklusionen er, at der er en trussel mod de danske energisektorer, og at et angreb mod de danske energisektorer kan have alvorlige konsekvenser.  Der ses et forøget antal cyberangreb mod kritisk infrastruktur internationalt over de seneste år, og der er ikke nogen antydning af, at dette vil ændre sig [12,13]. Endvidere er der set en udvikling i trusselsbilledet, hvor trusselsaktørerne angrebsmæssigt bevæger sig til andre enheder i det forsyningskritiske netværk og angriber nye komponenter i styringssystemerne. Komponenter, som man før angrebet ikke havde troet kunne angribes[10].

Det vurderes ud fra ROS-vurderingen og trusselsbilledet, at der stadig er et behov for en vedvarende strategi, som videreudvikler cyber- og informationssikkerheden inden for energisektorerne. Med udgangspunkt i en systematisk og metodisk proces er denne strategi for cyber- og informationssikkerhed et skridt i videreudviklingen af en sikker energiforsyning for Danmark, som bygger ovenpå det store arbejde, der allerede er gjort for at sikre en høj cyber- og informationssikkerhed i sektorerne.

# 4. Styrket nationalt samarbejde samt internationalt engagement

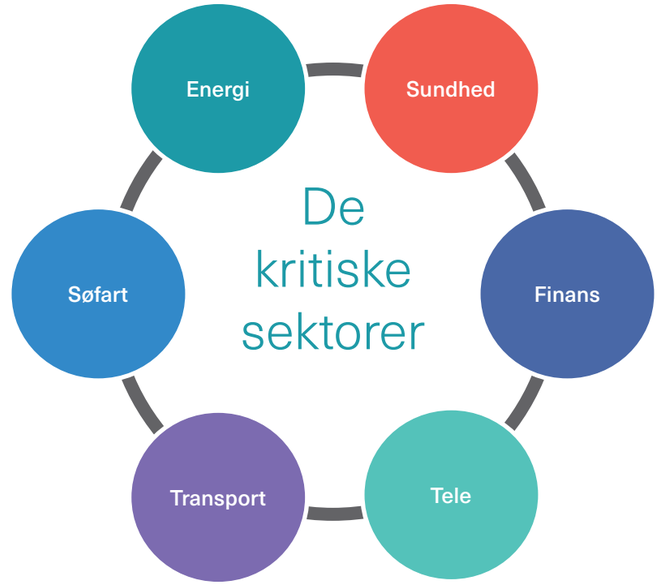
### Styrket nationalt samarbejde og koordinering

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.

Den myndighed, der har ansvaret for en opgave til dagligt, bevarer ansvaret under en hændelse

En del af den nationale cyber- og informationssikkerhedsstrategi vedrører etableringen af decentrale cyber- og informationssikkerhedsenheder (DCIS) hos hver af de samfundskritiske sektorer. DCIS-enhederne kan blandt andet bidrage til gennemførelsen af sektorvise trusselsvurderinger, beredskabsøvelser, sikkerhedsopbygning, vidensdeling, vejledning m.v. Denne enhed er per 1. juni 2018 implementeret i






*Figur 2: De kritiske sektorer*

Energistyrelsens organisation som en integreret del af Energistyrelsens eksisterende beredskabsenhed.

Det er væsentligt, at samarbejdet kan bruges før, under og efter en cyberhændelse

Samarbejde, videns- og kompetencedeling på tværs af de kritiske sektorer og med andre myndigheder, herunder CFCS, kan sikre det bedste grundlag for at bekæmpe cyberangreb. Det er væsentligt, at dette samarbejde kan bruges før, under og efter en cyberhændelse, og at de sektorspecifikke kompetencer tilgodeses. 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.

Samarbejdet på tværs kan medvirke til udveksling af informationer mellem sektorerne og de sektoransvarlige myndigheder. Informationsudveksling kan være vitalt for cybersikkerheden i en specifik sektor samt i tværsektorielle hændelser. Dette samarbejde bør have vidensdeling og erfaringsudveksling i højsædet.

### Internationalt udsyn og engagement

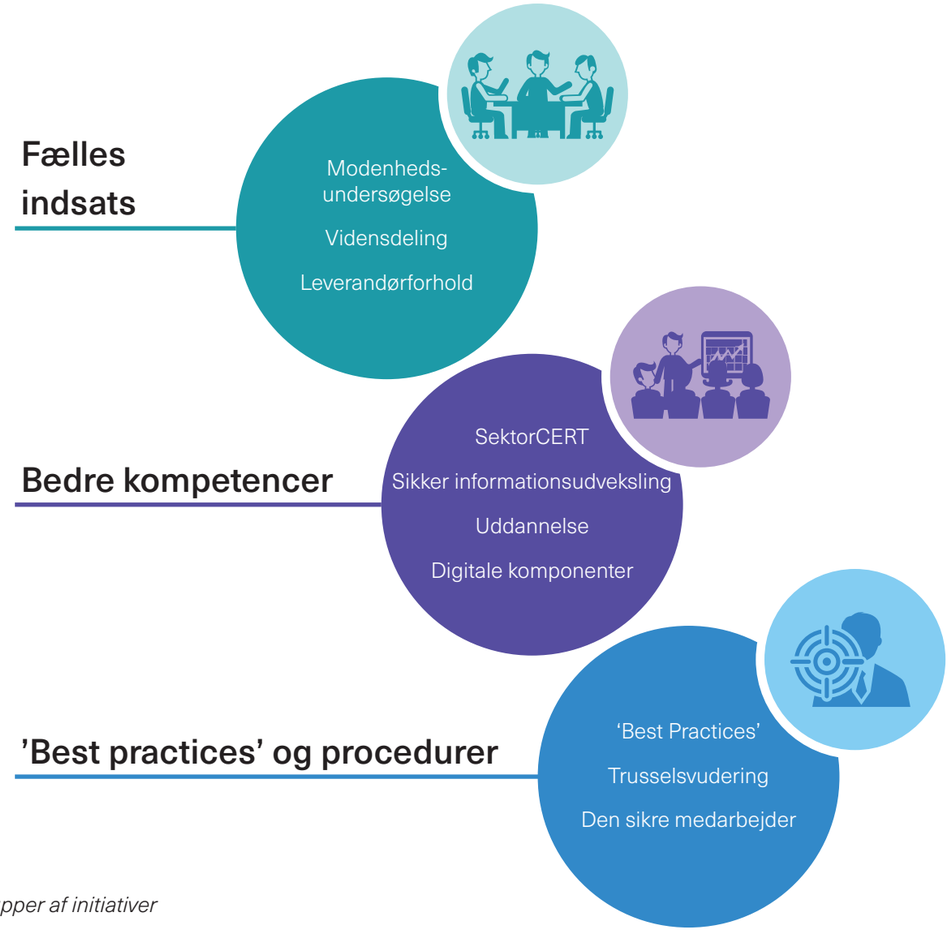
Informations- og cybersikkerhed i energisektorerne er højt på dagsorden i både EU og i resten verden. For at sikre at Danmark er bedst muligt rustet mod IT-relaterede angreb, er det afgørende, at både staten og sektorerne følger udviklingen uden for Danmark tæt, herunder indsamler erfaringer fra aktuelle angreb.

I de kommende år vil cyberområdet være højt prioriteret i EU. Cyberområdet har stor betydning for energi- og forsyningssikkerhed. Danmarks engagement i det internationale samarbejde skal derfor intensiveres ved at være stærkere repræsenteret i drøftelser i EU-, NATO- og FN-sammenhænge om cybersikkerhed.

# 5. Initiativer

For at staten og energisektorerne er forberedt bedst muligt på de udfordringer, som cyberangreb kan have på energisektorerne og derved fastholde den ønskede forsynings- og leveringssikkerhed, er der brug for nye initiativer.

Initiativerne er grupperet med udgangsgangspunkt i hovedemnerne i den nationale strategi vedrørende 'fælles indsats' og 'bedre kompetencer'. Derudover kommer i tillæg til dette en gruppering vedrørende 'best practices og procedurer'.




*Figur 3: De tre grupper af initiativer*


## 5.1. Fælles indsats

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 strategisk forankring af indsatser. Cyber- og informationssikkerheden i Danmark afhænger ikke blot af statens indsats på området, men i lige så høj grad af indsatsen i de samfundskritiske sektorer.

Energisektorerne består af en større mængde forskelligartede aktører, hvis baggrund, størrelse samt interne og lovmæssige forpligtigelser varierer afhængigt af forsyningsart og størrelse.

### INITIATIV 1 Systematisk og hyppig måling af modenhed og modstandsdygtighed

To elementer er centrale for at vurdere energisektorernes sikkerhedsniveau over for fx cyberangreb:

- **Modenhed** – dvs. i hvilken grad virksomheden har formaliseret og implementeret sikkerhedsprocesser, procedurer og kontroller for at styre cybersikkerheden i virksomheden.
- **Modstandsdygtighed** – dvs. i hvilken grad virksomheden er rustet til at håndtere fx et cyberangreb.

Som en del af den nationale strategi for cyber- og informationssikkerhed 2015-2016 [3] gennemførte Energistyrelsen i samarbejde med Energinet en vurdering af blandt andet sektorernes modenhedsniveau. Vurderingen viste, at energisektorernes modenhed og de implementerede sikkerhedskontroller er på et relativt højt sikkerhedsniveau sammenholdt med virksomheder i andre brancher. Energibranchen har et naturligt fokus på sikkerhed, hvilket blandt andet skyldes, at branchens primære opgave er at opretholde forsyningssikkerheden. Implementering af sikkerhedstiltag er dog ikke nødvendigvis foretaget med udgangspunkt i en formaliseret tilgang, hvor alle sikkerhedstiltag er lavet på basis af en aktiv stillingtagen til forretningens risiko. Samtidig viste vurderingen, at der er sammenhæng mellem virksomhedernes modenhed og deres størrelse. Der er ikke nogen systematisk plan eller lovkrav for udarbejdelse af vurderinger for modenhed og modstandsdygtighed.



Sektorernes modenhed og modstandsdygtighed skal ses i lyset af, at der er en hastig udvikling af cybertrusler, hvorfor trusselsbilledet løbende ændrer sig. Derfor vurderes det hensigtsmæssigt at vurdere modenheds- og modstandsdygtighedsniveauet hyppigt.

Selv om el- og naturgassektorerne har arbejdet systematisk med at styrke cyber- og informationssikkerheden, er det vurderingen, at sektorernes modenhed og modstandsdygtighed over for cybertrusler fortsat skal udvikles. Et centralt element er at tilvejebringe relevante data og dokumentation herfor med henblik på at skabe synlighed hos myndigheder, samfund og ledelse.

Initiativet vil belyse modenheden og modstandsdygtigheden mod cyberangreb på sektorniveau, men vil også kunne bruges af sektorernes virksomheder til at måle virksomhedens egen modenhed og modstandsdygtighed.

#### Anbefaling

Branchen gennemfører systematiske og hyppige vurderinger af modenheden og modstandsdygtigheden

Myndigheder og branchen udarbejder en ensartet metode for måling af modenheden og modstandsdygtigheden

| **Konkret skal initiativet:** |
|---|
| Udvikle et koncept for måling af modenhed og modstandsdygtighed, herunder udvikle en model, metode og proces til dannelse af datasæt ved brug af internationale standarder. |
| Fastsætte et anbefalet niveau for modenhed og modstandsdygtighed. |
| Gennemføre en selvstændig modenheds- og modstandsdygtighedsundersøgelse. |
| Etablere den fremtidige proces for gennemførsel af hyppige modenheds- og modstandsdygtighedsmålinger. |
| Anbefale hvor ofte en modenheds- og modstandsdygtighedsanalyse bør laves hos virksomhederne. |

| Succeskriterier |
| --- |
| Der er udviklet en model for måling af modenhed og modstandsdygtighed med udgangspunkt i anerkendte internationale metodestandarder, som indeholder et anbefalet niveau for modenhed og modstandsdygtighed. |
| Målingen af modenhed og modstandsdygtighed giver, sammen med det lovpligtige tilsyn, myndigheder grundlag for at vurdere, hvordan sektorerne er sikret mod forventede cybersikkerhedshændelser. |
| Måling af modenheden og modstandsdygtigheden samt det lovpligtige tilsyn skaber øget fokus internt i energivirksomheder på cybersikkerhed. |



# INITIATIV 2 Styrket vidensdeling

Hurtig, relevant og præventiv vidensdeling om cybertrusler er vigtig for, at sektorernes virksomheder kan etablere den nødvendige beskyttelse. Ved i tide at indhente relevante samt operationelt vigtige informationer, herunder fra CFCS, vil sandsynligheden for at undgå eller mitigere konsekvenserne ved et cyberangreb øges væsentligt. Derfor er det vigtigt, at den allerede erkendte viden fra eksisterende kompetencer og kilder i staten og sektorerne kan spredes på en effektiv, systematiseret og fortrolig måde til gavn for de samlede nationale energisektorer.

Deling af viden foregår i dag i vid udstrækning inden for energisektorerne, hvilket er en af sektorernes styrker. I forhold til cybersikkerhed er der dog mange virksomheder, som individuelt skal løfte en relativt stor opgave med at holde sig opdateret med vigtige, proaktive tiltag. For større virksomheder kan der være råderum til at arbejde i dybden med enkelte relevante emner, men der er ikke nødvendigvis ressourcer til at deltage i alle aktiviteter og netværk for hver eneste aktør. Grundet kompleksiteten inden for cybersikkerhed er der fortsat behov for at udvikle vidensdelingen internt i sektorerne.

Viden om cybersikkerhed i staten er spredt på flere myndigheder, og det vurderes hensigtsmæssigt med klare procedurer for, hvordan viden og erfaring deles internt mellem myndigheder. Samtidig bør der etableres klare procedurer for vidensdeling mellem myndigheder og branchen.

Initiativet skal tilvejebringe og fremme gensidig deling af relevant viden samt bistå den tværgående indsats i den nationale strategi i relation til samfundskritiske aktører under andre myndigheders ressort.

## Anbefaling

Der etableres klare procedurer for vidensdeling mellem myndighederne

Der etableres klare procedurer for vidensdeling mellem myndighederne og energisektorernes aktører

Der etableres klare procedurer for vidensdeling internt mellem energisektorernes aktører

| Konkret skal initiativet: |
|---|
| Afdække behovet for vidensdeling blandt de forskellige aktører i energisektorerne. |
| Afdække behovet for vidensdeling på tværs af og med de andre samfundskritiske sektorer samt nationale beredskabs- og sikkerhedsmyndigheder. |
| Kortlægge anvendte aktørers fora, netværk med videre, således at der dannes et systematiseret overblik over den eksisterende vidensdeling. |
| Udarbejde en metode for vidensdeling, som også muliggør fortrolighed og konstruktiv åbenhed. |
| Etablere en anbefalet proces for effektiv vidensdeling, som vil lette adgangen til relevant viden. |
| Kortlægge behovet for en fælles vidensbank af dokumenter, netværksgrupper, fora og lignende, hvor der i bred åbenhed inden for energisektorerne deles relevant viden. |
| Danne overblik over, hvordan der sikres god kvalitet af viden og niveauer. |

| Succeskriterier |
|---|
| Behovet for vidensdeling i sektorerne er afdækket og er bredt understøttet af energivirksomhederne. |
| Der er etableret relevant og prioriteret vidensdeling på tværs af samfundskritiske sektorer. |
| Der er etableret effektive processer for vidensdeling inden for energisektorerne og mellem myndighederne. |

## INITIATIV 3 Krav til leverandørforhold

Inddragelse af leverandørforhold er et fokusområde i den nationale cyber- og informationsstrategi 2018-2021, hvilket indebærer, at der er styr på leverandører af samfundskritisk IT. I energisektorerne er der – som i andre sektorer – en række underleverandører af samfundskritisk IT. De samfundskritiske systemer består af fysisk udstyr og software leveret af kommercielle virksomheder, der lever af et marked inden for industrielle kontrolsystemer, og som udgør en vital del af infrastrukturen bag den nationale forsyning af energi.



Der findes i dag ikke systematiske krav til cybersikkerhed til leverandører. Det er ejeren af en energivirksomhed, der er ansvarlig for sikkerheden af virksomhedens systemer. Kæden af leverandører, ydelser og fysisk udstyr er meget kompleks, og tidligere undersøgelser [14, 15] har vist, at der er konkrete risici og forhold forbundet med leverandørerne til virksomhederne og de indbyrdes samarbejdsrelationer.

Initiativet skal lette og forbedre arbejdet med kontrakter og videre samarbejde om udvikling af produkter mellem leverandør og energivirksomheder ved, at disse fremadrettet kan tage udgangspunkt i en række 'best practices' udarbejdet som en del af initiativet for at øge cybersikkerheden i øverste led af 'supply chain' – både for leverandør og energivirksomheder. Forankring af initiativet blandt deltagende parter sker ved, at der ikke ændres på energivirksomheders ansvar, men at der i fællesskab etableres nogle muligheder for at forenkle processerne omkring håndtering af leverandører, og at leverandører oplever en tilsvarende forenklet proces hos de energivirksomheder, som vælger at læne sig op ad 'best practices'.

Rammerne for initiativet er delt op i to faser: 1) Energistyrelsen udarbejder en analyse af forretningsforhold mellem energivirksomheder og leverandører i relation til cybersikkerhed. Analysen baseres blandt andet på et eksisterende nordisk samarbejde, hvor Norge og Danmark har gennemført interviews af leverandører og virksomheder. 2) Branchen udarbejder 'best practices' baseret på sektorernes eksisterende erfaringer. Initiativet skal endvidere give input til videre arbejde med standarder i internationalt regi, herunder ENISA (European Union Agency for Network and Information Security) i EU og IEA (International Energy Agency) i samarbejde med branchen.

## Anbefaling

Energistyrelsen udarbejder en analyse af forretningsforhold mellem energivirksomheder og leverandører i relation til cybersikkerhed

Branchen udarbejder best practice for krav til cybersikkerhed til leverandører

Der arbejdes efter at anvende eller alternativt videreudvikle internationale standarder for krav til leverandører

**Konkret skal initiativet:**

Undersøge fordele og ulemper ved at indføre audit og certificering af givne produkttyper.

Undersøge energivirksomhedernes afhængighed af leverandører.

Udarbejde en anbefaling til fælles krav ved outsourcing af driften.

Undersøge grundlaget for standardkontrakter som kan benyttes og arbejdes videre med.

Afdække og komme med anbefaling til 'best practices' for krav til leverandører.

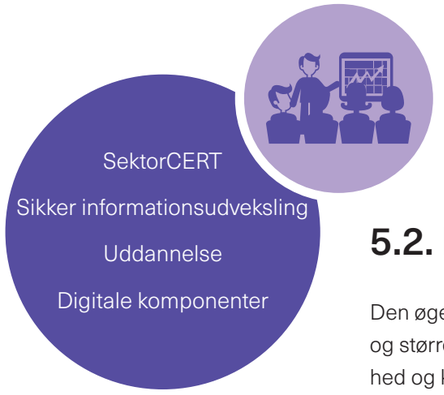
**Succeskriterier**

Cybersikkerhed indgår som en naturlig integreret del af kontraktindgåelse mellem energivirksomheder og deres leverandører.

Der er international koordinering (fx i Norden eller EU) om krav til cybersikkerhed til leverandørerne.

Der er udarbejdet 'best practices', som er relevante for danske energivirksomheder.






## 5.2. Bedre kompetencer

Den øgede digitalisering og konstante forandring i trusselsbilledet stiller større og større krav til myndighedernes og energisektorernes 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 viden om cyber- og informationssikkerhed øges.

### INITIATIV 4 SektorCERT

Den stigende trussel mod cyber- og informationssikkerhed stiller nye krav til myndigheder og branchen i forhold til at dele viden (fx om hændelser og angreb), monitorere udviklingen i energisektorerne, vurdere trusselsbilledet, komme med relevante varslinger, stille beredskab og 'best practices' til rådighed, når hændelsen er sket samt rådgive og uddanne medarbejdere og ledelse. Cyber- og informationsudfordringen er ofte så stor og kompleks, at kun de største virksomheder kan løfte opgaven. I andre lande – blandt andet Norge og USA – har man etableret et sektorspecifikt kompetencecenter – en såkaldt sektorCERT (Computer Emergency Response Team), hvilket er en IT-sikkerhedstjeneste, som i forskelligt omfang vil kunne samle kompetencerne inden for informations- og cybersikkerhed, og som derved vil kunne rådgive branchen og myndigheder.

Det vurderes, at en sådan sektorCERT med sektorspecifikke kompetencer er relevant for energisektorerne for at kunne agere professionelt på cybertruslen mod energisektorerne. Det udestår, hvordan en sektorCERT kan etableres, heriblandt organisation, ejerskab og finansiering af en sektorCERT for energisektorerne. Initiativet vil undersøge, hvordan en sektorCERT vil kunne etableres, og hvorvidt der inden for energisektorerne er et grundlag for at etablere en fælles sektorCERT med specialistkompetencer inden for cybersikkerhed i energisektorerne, samt hvordan et eventuelt samarbejde herom mellem myndigheder og sektorerne skal fungere.

En sektorCERT vil, afhængig af opbygningen heraf, kunne bidrage med specialiseret viden og erfaringsbaserede kompetencer på ydelser som fx rådgivning og undervisning, cybersikkerhedsinformationer og konsulentassistance til

sektorerne og myndigheder før, under og efter hændelser. Myndighedernes konkrete rolle og bidrag til en sådan sektorCERT vil i givet fald skulle defineres meget præcist.

## Anbefaling

Der arbejdes for etablering af en sektorCERT i samarbejde med sektorerne

| Konkret skal initiativet: |
|---|
| Udarbejde et beslutningsgrundlag for etablering af en sektorCERT. |
| Afdække mulig organisering, ejerskab, finansiering og governance af en sektorCERT for energisektorerne. |
| Udarbejdelse af tidsplan og budget for etableringen af en sektorCERT. |
| Foretage en kortlægning af samarbejdsforhold mellem en sektorCERT, sektorerne og myndighederne fx Center for Cybersikkerhed, Energistyrelsen og Energi-, Forsynings- og Klimaministeriets departement. |
| Fastlægge mulige, relevante ydelser fra en sektorCERT. |
| Afdække vigtige samarbejdspartnere nationalt og internationalt for en sektorCERT. |
| Afdække muligheden for "Public Private Partnership" for en sektorCERT. |

| Succeskriterier |
|---|
| Der er etableret et beslutningsgrundlag til brug for vurdering af, hvordan der kan etableres en sektorCERT. |
| Organisation, governance, finansiering og ejerskab for en sektorCERT er grundigt udarbejdet i tæt samarbejde med myndigheder og energisektorerne. |
| Der er udarbejdet en oversigt over eksisterende IT-sikkerhedstjenester i Danmark. |
| Der er udarbejdet en grundig analyse og efterfølgende anbefaling til, hvordan samarbejde mellem myndigheder og sektorerne kan og bør foregå. |
| Grundlaget for de væsentlige ydelser, som en sektorCERT kan og bør levere, er afdækket i tæt samarbejde med energisektorerne. |



# INITIATIV 5 Sikker informationsudveksling

Aktører i energisektorerne har behov for hyppig indbyrdes kommunikation vedrørende energidata for at kunne opretholde både en stabil forsyning og drive en fornuftig forretning. Et centralt punkt for cybersikkerhed generelt er at kunne håndtere udvekslingen af informationer på en sikker måde, hvilket også gælder i energisektorerne.

Håndteringen af sikker udveksling af informationer afstedkommer et behov for at videreudvikle IT-arkitekturen (blandt andet IT-systemerne) baseret på internationalt anbefalede standarder. En gennemtænkt IT-arkitektur er et vigtigt led i god cyber- og informationssikkerhed.

Initiativet drives af branchen og bør tilgodese store og små virksomheder samt de nuværende og kommende IT-arkitekturer og løsninger inden for energisektorerne. Initiativet skal endvidere baseres på eksisterende nationale og europæiske beslutninger om sikker standardiseret informationsudveksling.

## Anbefaling

Branchen vil udarbejde standarder for sikker informationsudveksling

| Konkret skal initiativet: |
|---|
| Kortlægge og anbefale relevante standarder for sikker informationsudveksling. |
| Analysere 'best practises' og udarbejde en vejledning for god opbygning og brug af netværksarkitektur og udveksling af informationer. |
| Foretage vurdering af i hvilken grad IT-komponenter, IT-services og software udgør byggestenene i en forsyningskritisk IT-infrastruktur for informationsudveksling. |
| Kortlægge og anbefale brug og håndtering af certifikater til brug for kryptering og autentifikation af aktører og IT-systemer, der er kendte, som en væsentlig faktor i globale IT-infrastrukturer, fra luftfartsområdet til finans- og sundhedsvæsen. |

| Succeskriterier |
| --- |
| Initiativet sikrer en effektiv brug af internationale standarder for effektiv informationsudveksling, således at kommunikation foregår på en sikker og standardiseret måde på tværs af danske energivirksomheder. |
| Informationsudveksling sker på et højt modenhedsniveau ved sammenligning med energisektorer i internationalt regi. |




# INITIATIV 6 Uddannelse

Uddannelse er et fokusområde i den nationale cyber- og informationsstrategi 2018-2021. Uddannelse og efteruddannelser inden for sektorerne med fokus på cybersikkerhed er et grundelement for at øge cybersikkerheden på både kort og lang sigt.

Et vedholdende højt niveau af cybersikkerhed kræver både ledelsesbevågenhed og tilstrækkelig viden hos medarbejdere i virksomheden. Mange virksomheder gennemfører derfor i dag løbende 'awareness-kampagner' for deres medarbejdere. Der er samtidig en løbende risikostyring, der sikrer, at cybersikkerhed er på dagsordenen i virksomhedernes topledelser.

Energisektorerne skal dog fortsat sikre, at cybertruslen fastholdes i bevidstheden hos virksomhedernes topledelser, og at medarbejderne tilegner sig tilstrækkelig viden.

Studerende med interesse for cybersikkerhed bliver ikke altid introduceret til energisektorernes område og cybersikkerhedens betydning for opretholdelse af energiforsyningen. Andre samfundskritiske sektorer kan opleve samme udfordring med at rekruttere de nødvendige kompetencer. Der er i dag markant fokus på IT og OT (Operational Technology) hørende til forskellige faggrupper.

## Anbefaling

Den sektorspecifikke uddannelse og efteruddannelse skal styrkes

| Konkret skal initiativet: |
| --- |
| Analysere det specifikke uddannelses- og efteruddannelsesbehov i energisektorerne samt komme med en anbefaling om, hvem der kan udbyde videre tiltag om dette. |
| Kortlægge hvilke relevante uddannelser og efteruddannelser der allerede eksisterer. |
| Kortlægge hvilke uddannelser der aktivt bruges i sektorerne i dag. |
| Udarbejde en plan for etablering af tværsektorielt samarbejde og samarbejde med uddannelsesinstitutioner for at fremme cybersikkerhed i energisektorerne. |

**Succeskriterier**

Der er sikret et effektivt og fagligt funderet beslutningsgrundlag for, hvordan arbejdet med cybersikkerhed i uddannelsesregi kan opnå synergieffekter i relation til energibranchen.

Der er etableret et tværsektorielt samarbejde og overblik vedrørende relevante uddannelser og det videre arbejde med disse, således at initiativet er medvirkende til at kunne give input til uddannelsesinstitutioner i samarbejde med øvrige myndigheder.


## INITIATIV 7 Sikring af digitale komponenter – Industrial IoT

En del af digitaliseringen i energisektorerne er implementeringen af en ny type enheder kendt som IIoT (Industrial Internet of Things) eller Industri 4.0. Implementering af IIoT i de kritiske netværk er et led i effektiviseringen af processer og giver blandt andet et bedre overblik over systemer. IIoT er en undergruppe til det mere kendte IoT (Internet of Things), som kendetegnes ved alverdens IT-udstyr, som kan kobles til internettet.



Energisektorerne har påbegyndt den øgede digitalisering, og det forventes at inkludere de forsyningskritiske netværk. Brugen af IIoT i energiforsyningen kan have en konsekvens for cybersikkerheden, da mange IoT- og IIoT-enheder ikke har implementeret tilstrækkelige cybersikkerhedsfunktioner.

Initiativet skal via 'best practices' udpege vigtige forhold i sektorerne i forhold til at øge cybersikkerheden, specielt omkring brugen af IIoT i de kritiske netværk og løsninger. Grundlæggende sikkerhedsdesign (Security by design) vil i den sammenhæng blive et vigtigt tema og fokusområde for energisektorerne.

### Anbefaling

Branchen skal udarbejde 'best practices' for digitale komponenter (IIoT)

**Konkret skal initiativet:**

Afdække risici ved anvendelse af IIoT-løsninger i kritisk infrastruktur.

Kortlægge 'best practises' internationalt for vurdering og udvælgelse af leverandører, som skal levere digitale produkter til kritisk infrastruktur.

Præsentere forslag til 'best practices' vedrørende implementering af IIoT til anvendelse i den kritiske infrastruktur.

Skitsere samarbejdsmuligheder med andre myndigheder, organisationer og virksomheder og leverandører omkring IIoT.

Kortlægge behov, fordele og ulemper ved aktiv deltagelse i internationale standardiseringsfora.

Kortlægge certificeringsordninger, der findes inden for IIoT i internationalt regi.

**Succeskriterier**

Der er sikret et overblik over, hvordan IIoT-løsninger anvendes i kritisk infrastruktur.

Der er bidraget til en øget synliggørelse og konkrete 'best practices' til brug for energivirksomheder vedrørende effektiv og fremtidssikret stillingtagen til metoder bag vurderingen af, hvorledes IIoT-løsninger kan benyttes, og hvilke risici der bør overvejes i den relation.



‘Best Practices’

Trusselsvudering

Den sikre medarbejder

## 5.3. ’Best practices’ og procedurer

Der findes områder, hvor rammerne, standarder og mulige procedurer er kendte i forvejen, men hvor der ikke i udpræget grad er synkroniseret processer og procedurer i fællesskab hen over energisektorerne. Det vurderes muligt at øge sektorernes cybersikkerhed ved øget anvendelse af ’best practices’ og ved at anvende mere effektive procedurer.

### INITIATIV 8 Standarder og’ best practices’

Det er i høj grad op til den enkelte virksomhed at leve op til interne og eksterne krav til informations- og cybersikkerhed – herunder ligger også myndighedskrav. Dette er særligt en udfordring for sektorernes mindre aktører.

For at energisektorernes virksomheder får et mere ensartet grundlag til fx at designe og indkøbe IT/OT-systemer er der behov for at udvikle branchestandarder og dele viden om de bedste metoder til at håndtere cyberudfordringerne. Branchestandarder (fx minimumskrav til indkøb af IT-løsninger) og ’best practices’-anbefalinger kan således bidrage til at hæve modenheden og modstandsdygtigheden i energisektorerne med henblik på at sikre, at alle virksomheder lever op til et minimumssikkerhedsniveau.

Initiativet skal forankres bredt i energisektorerne og bør baseres på kendte standarder og konkrete erfaringer. Er der tale om nye tiltag, hvor der mangler det længerevarende erfaringsmæssige grundlag, er det væsentligt, at dette er erkendt under arbejdet, så det sikres, at der på sigt skabes solidt funderede ’best practices’.

#### Anbefaling

Branchen bidrager med branchestandarder og anbefalinger til at dele ’best practices’

**Konkret skal initiativet:**

Undersøge, hvilke nationale og internationale 'best practices' og branchestandarder, der kan bruges til at øge modenheden og modstandsdygtigheden i energisektorerne, inklusive praktiske erfaringer fra andre sektorer og lande.

Vurdere og anbefale, hvilket indhold der passer til sektorerne, baseret på kvalitative interviews med relevante aktører i de danske energisektorer samt kommunikation med andre relevante nationale samfundskritiske sektorer og udenlandske aktører.

Etablere standarder i faglig dialog og sparring mellem forskellige sektorer, myndigheder, universiteter og øvrige faglige input i internationalt regi.

**Succeskriterier**

Der er udarbejdet branchestandarder for relevante områder.

'Best practices' er udarbejdet med udgangspunkt i internationalt bredt anerkendte standarder og medvirker til et øget internationalt samarbejde og forenklede processer for leverandører til energisektorerne i gensidig interesse.

'Best practices' er rettet mod flere typer og størrelser af energivirksomheder og gør, at den enkelte virksomhed kan tilpasse sit arbejde ud fra virksomhedens størrelse og kompleksitet.

Initiativet bidrager til en forøget dialog og synlighed i samarbejdet mellem myndigheder og sektorerne.



# INITIATIV 9 Styrket grundlag for trusselvurderinger

CFCS udsender årlige trusselvurderinger for energisektorerne vedrørende risikoen for cyberangreb fra fremmede magter. CFCS' trusselvurdering suppleres af en ROS-vurdering, som udarbejdes årligt for el- og naturgassektorerne, som en del af bekendtgørelsen om IT-beredskab for el- og naturgassektorerne – jf. afsnit 3.

Trusselvurderingerne er vigtige for, at sektorerne kan forebygge cyberangreb. Derfor skal det afdækkes, hvilke informationer der skal indgå i vurderingerne, og hvor hyppigt de skal udarbejdes.

For at sikre at trusselvurderingerne er baseret på de mest opdaterede og troværdige kilder, er det afgørende, at trusselvurderingerne baseres på en systematisk metode, anerkendte kilder og effektiv vidensdeling mellem myndigheder og sektorerne om udviklingen om cybertruslerne mod energisektorerne.

## Anbefaling

Viden og kilder til brug for trusselvurderinger skal systematiseres

**Konkret skal initiativet:**

Afdække det konkrete behov for information om cybertruslen, herunder hvilket format og detaljeindhold der er relevant for virksomhederne.

Afdække, hvilke kilder som bør og kan lægges til grund for den udsendte information.

Afdække med hvilken frekvens information bør udsendes og indsamles.

Afklare, hvem der leverer hvilken information mellem sektorerne og CFCS.

Afdække gennem hvilke kanaler information bør formidles.

Afklare, hvem der kan forestå jævnlige udsendelser af en "cybervejrudsigt".

Afklare, hvordan kvalitet og validering af information kan sikres.

**Succeskriterier**

Initiativet sikrer en effektiv løbende trusselsvurdering under hensyntagen til de risici og sårbarheder, der eksisterer i energisektorerne.

Initiativet udarbejdes i tæt dialog med CFCS og øvrige myndigheder, således at der er klare snitflader mellem, hvilke parter der bidrager med hvilke dele af den samlede trusselsanalyse.

Der anvendes internationale såvel som nationalt anerkendte kilder til vurdering af trusler mod sektorerne.

Der er etableret klare snitflader i forhold til trusselsvurderinger om forsyningskritiske IT-systemer og mere generelle IT-systemer, således at trusselsvurderingernes omfang er veldefineret.

## INITIATIV 10 Den sikre medarbejder

Medarbejdere, der betjener og opsætter IT-systemerne og netværk, er en væsentlig faktor for cybersikkerheden i forsyningskritiske netværk. Korrekt uddannelse og løbende træning mindsker risikoen for fejl. Derfor er det vigtigt, at der er klare procedurer for sikkerhedsgodkendelse af personer, som arbejder med eller har adgang til forsyningskritisk materiale. Samtidig skal der være klare procedurer for, hvilke medarbejdere, som har adgang til bestemte IT-systemer. Endelig er det afgørende løbende at træne medarbejderne, blandt andet via løbende 'awareness-øvelser'.

### Anbefaling

Myndigheder og virksomheder skal have klare procedurer for sikkerhedsgodkendelse af medarbejdere

Myndigheder og virksomheder skal have klare retningslinjer for, hvem der har adgang til hvilke IT-systemer

Myndigheder og virksomheder skal løbende 'awareness-træne' medarbejdere

**Konkret skal initiativet:**

Afdække praksis for sikkerhedsgodkendelse af personer.

Udarbejde konkrete anbefalinger til processen for sikkerhedsgodkendelse.

Afdække praksis for 'awareness-træning' af medarbejdere.

Udarbejde konkrete anbefalinger til processen for 'awareness-træning'.



**Succeskriterier**

Myndigheder og virksomheder har gennemført undersøgelser af eksisterende sikkerhedsgodkendelser og træning af medarbejdere.

Der er løbende 'awareness-træning' af medarbejdere i myndigheder og virksomheder.

Der er udarbejdet anbefalinger for sikkerhedsgodkendelse af personer i myndigheder og virksomheder.

Cyber- og informations-sikkerhedspro-grammet gen-nemfører de 10 initiativer

## 5.4. Program og tidsplan

For at følge, evaluere og styre processen for implementeringen af de 10 initiativer i cyber- og informationssikkerhedsstrategien for energisektorerne bliver der lavet et cyber- og informationssikkerhedsprogram. Cyber- og informationssikkerhedsprogrammet etableres i Energistyrelsen med en styregruppe og en programledelse. Cyber- og informationssikkerhedsprogrammet har til formål at styre og sikre en effektiv gennemførelse af de 10 initiativer i cyber- og informationssikkerhedsstrategien for energisektorerne.

De enkelte initiativer bliver udført som projekter med involvering af branchen og vil referere til cyber- og informationssikkerhedsprogrammet, som også styrer den overordnede tidsplan. Initiativernes start- og sluttid er planlagt over strategiperioden fra 2018 – 2021. I programmets tidsperiode vil der blive etableret en midtvejsevaluering ud over de periodiske styregruppemøder.

# 6. Bilag

Bilag A

## Bilag A: Metode

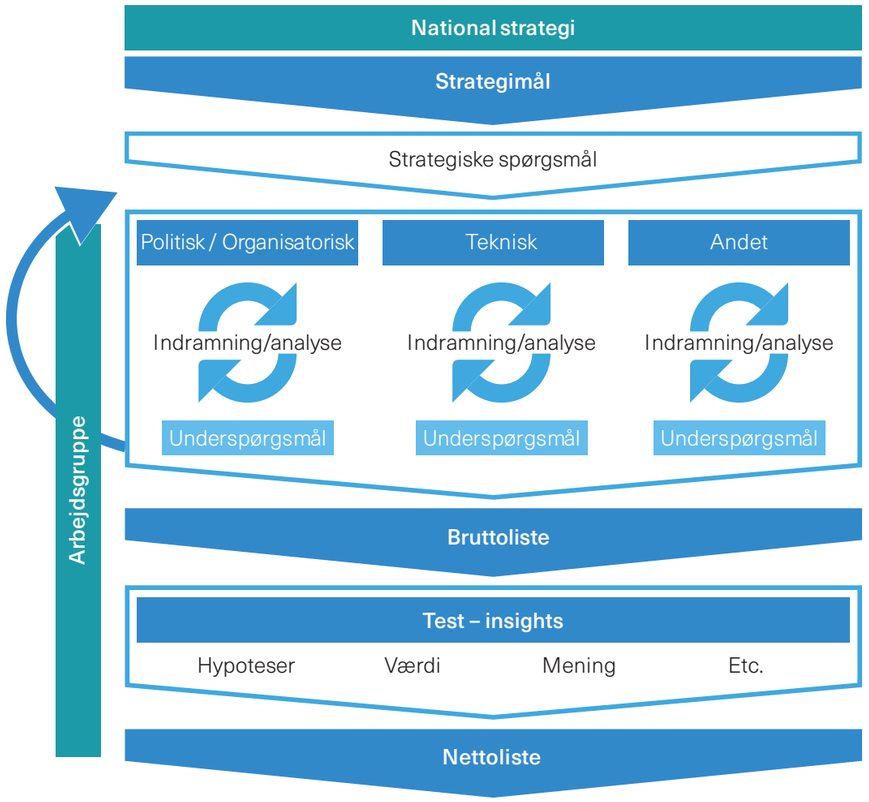
Cyber- og informationssikkerhedsstrategien for energisektorerne er udarbejdet ud fra en systematisk og metodisk proces. Fokus har været på at sikre informationer, at effektivisere arbejdet og at kunne levere en strategi med høj kvalitet, som efterfølgende kan implementeres og bruges som en vedvarende strategi.

I udarbejdelsen af cyber- og informationssikkerhedsstrategien for energisektorerne har der været en stor involvering af sektorerne med henblik på at øge kvaliteten af strategien samt at integrere og belyse de udfordringer, som virksomhederne og myndigheder har omkring cybersikkerhed i de forsyningskritiske netværk og systemer.

Udarbejdelsen af cyber- og informationssikkerhedsstrategien for energisektorerne er blevet etableret som et projekt med styre- og arbejdsgruppe. Styregruppen har bestået af Energi-, Forsynings- og Klimaministeriets departement, Energistyrelsen, Energinet og Dansk Energi. Arbejdsgruppen har inkluderet repræsentanter for Energi-, Forsynings- og Klimaministeriets departement, Energistyrelsen, Energinet, Dansk Energi, Dansk Fjernvarme, Radius, HOFOR og Dinel.

Projektet blev startet i maj 2018 med udarbejdelsen af et kommissorium, som har styret hovedlinjerne i projektet.

Projektets arbejdsgruppe har overordnet arbejdet ud fra en modificeret strategimodel[16], som er vist i figur 4 på næste side.




*Figur 4: Arbejdsgruppens strategimodel*

Denne model er benyttet til at udarbejde, vurdere og kvalificere initiativerne i strategien for energisektorerne, som har taget udgangspunkt i den nationale strategi for cyber- og informationssikkerhed 2018-2021 og kommissoriet for projektet.  Modellen deler arbejdsgruppens arbejde op i delopgaver og områder med henblik på at sikre en systematisk arbejdsmodel for arbejdet med udviklingen af strategiens initiativer. Modellens to hovedområder er en brutto- og nettoliste af initiativer og elementer til den strategiske tænkning for at udarbejde disse lister. Bruttolisten af initiativer blev efterfølgende diskuteret og vurderet på en workshop, hvor et bredt udsnit af sektorernes virksomheder deltog. Arbejdet blev afsluttet med arbejdsgruppens udvælgelse af 10 initiativer til at øge cyber- og informationssikkerheden i energisektorerne med udgangspunkt i den nationale strategi eller kommissoriet for projektet. Initiativerne er efterfølgende blevet vurderet og kvalificeret af arbejdsgruppen.

Initiativerne i cyber- og informationssikkerhedsstrategien for energisektorerne er struktureret ud fra tre hovedemner: fælles indsats, bedre kompetencer samt 'best practices' og procedurer, samt de effektområder de enkelte initiativer vil have indvirkning på. Disse effektområder bygger på en cybersikkerhedshændelsesproces og er defineret som før, under og efter en hændelse.



Bilag B

# Bilag B: Referencer

[1] Finansministeriet, National strategi for cyber- og informationssikkerhed, 2018

[2] ICS-CERT, IIOT and the Cyber Threat: A Perfect Storm of Risk, 2017

[3] Finansministeriet, National strategi for cyber- og informationssikkerhed, 2014

[4] SANS, Analysis of the Cyber Attack on the Ukrainian Power Grid, 2016

[5] ZDNET, www.zdnet.com/article/industroyer-an-in-depth-look-at-the-culprit-behind-ukraines-power-grid-blackout/ [tilgået 13.11.2018], 2018

[6] CFCS, Undersøgelsesrapport – Målrettede forsøg på hacking af den danske energisektor, 2018

[7] CFCS, Cybertruslen mod energisektoren, 2018

[8] ESET, Greyenergy a successer to BlackEnergy, 2018

[9] NCCIC, Russian government cyber activity targeting energy and other critical infrastructure sectors, 2018

[10] Dragos, TRISIS Malware, Analasis of Safty System Targeted Malware, 2018

[11] SANS, The industrial control system cyber kill chain, 2015

[12] Verizon, Data breach investigations report, 2017

[13] Verizon, Data breach investigations report, 2018

[14] PWC, Forundersøgelse af modenheds- og sikkerhedsniveauet indenfor cyber- og informationssikkerhed blandt danske el- og naturgasselskaber, 2015

[15] NVE, Informationssikkerhedstilstanden i energiforsyningen, (Norge), 2017

[16] Tovstiga, G, Strategy in practice, 2010

# Cyber- og informationssikkerhedsstrategi for energisektorerne

Udgivet januae 2019

Henvendelse om publikationen kan ske til:

**Energistyrelsen**
Amaliegade 44
1256 København K
Tlf.: +45 33 92 67 00

ISBN Elektronisk publikation 978-87-93180-38-3
Publikationen kan hentes på www.ens.dk

Grafik og layout: Solid Media Solutions