Energistyrelsen

Cyber- og informations-sikkerhedsstrategi for el-, gas- og fjernvarmesektorerne 2022-2025

Energistyrelsen
Carsten Niebuhrs Gade 43
1577 København V

Telefon: 33 92 67 00
E-mail: dcis-energi@ens.dk
www.ens.dk

Indhold

Indledning

Regeringen offentliggjorde d. 15. december 2021 en ny national strategi for cyber- og informationssikkerhed for perioden 2022-2024. Strategien præsenterer fire centrale målsætninger for det fremadrettede arbejde med cyber- og informationssikkerhed:

Robust beskyttelse af de samfundsvigtige funktioner

Styrkelse af det offentligt-private samarbejde

Øget kompetenceniveau og ledelsesforankring

Aktiv deltagelse i den internationale kamp mod cybertruslen

Denne strategi for cyber- og informationssikkerhed i energisektorerne er Energistyrelsens bidrag til den nationale strategiske indsats for cyber- og informationssikkerhed og følger af det nationale krav om, at der formuleres delstrategier for arbejdet med cyber- og informationssikkerhed i de samfundsvigtige sektorer. Regeringen har med den nye nationale strategi for cyber- og informationssikkerhed sat fokus på at højne cybersikkerheden i den kritiske infrastruktur. I overensstemmelse med den dagsorden er formålet med sektorstrategien at højne cyber- og informationssikkerheden i energisektorerne, så fordelene ved bl.a. digitaliseringen kan udnyttes

– særligt i omstillingen til mere grøn og vedvarende energi – samtidigt med, at truslerne fra cyberspace håndteres på forsvarlig vis.

Det danske energisystem er under hastig omstilling bl.a. som følge af Klimalovens målsætninger om, at Danmark i 2030 skal reducere udledningen af drivhusgasser med 70 pct. i forhold til niveauet i 1990 og opnå klimaneutralitet senest i 2050. Den grønne omstilling betyder, at bl.a. el-, gas- og fjernvarmesystemerne står overfor væsentlige forandringer. En omfattende elektrificering af det danske energisystem er en hjørnesten i at indfri målsætningerne. Også varmesektoren skal gennemgå en gennemgribende omstilling og elektrificering, så de fossile brændsler kan udfases. Det samme gælder transportsektoren, hvor den tunge trafik (særligt skibe og fly) skal anvende syntetiske brændstoffer fra power-to-x. Endelig skal industrien elektrificeres mest muligt, så fossile brændsler og biogas målrettes de sektorer, der ikke kan elektrificeres – f.eks. højtemperaturprocesser. En smart og vellykket omstilling til mere vedvarende energi går hånd i hånd med digitalisering af energisektorerne. Derfor er det afgørende, at sektoren er bedst muligt forberedt på nuværende og fremtidige trusler fra cyberspace – og derfor sætter denne strategi fokus på cybersikkerheden i disse sektorer.

En sikker og stabil energiforsyning er en forudsætning for et velfungerende samfund, og i Danmark har vi et af verdens højeste niveauer af forsyningssikkerhed. Det skal der holdes fast i. Også under omstillingen til grøn energi og den samtidige digitalisering af energisystemet.

Markant og kompleks cybertrussel i forandring

De danske energisektorer står, som resten af det danske samfund, overfor alvorlige trusler fra cyberspace. Cybertruslen drives af, at cyberkriminelle, statssponsorerede hackergrupper og efterretningstjenester forsøger at udnytte digitaliseringen af alle dele af samfundet. Med digitaliseringen følger nemlig flere sårbarheder, som muliggør cyberkriminalitet, cyberspionage og destruktive cyberangreb.

Truslen imod energisektorerne fra cyberspionage og cyberkriminalitet i form af ransomware-angreb vurderes af Center for Cybersikkerhed (CFCS) at være meget høj. Som et foregangsland inden for energisikkerhed og overgangen til grøn energi og et knudepunkt i det europæiske el- og naturgasnet er den danske energisektor interessant for fremmede stater. Sektoren står samtidigt over for truslen fra cyberkriminelle i form af både målrettede angreb

De danske energisektorer står, som resten af det danske samfund, overfor alvorlige trusler fra cyberspace

og angreb rettet mod et stort antal personer, såsom phishing. De mulige konsekvenser ved operationelle driftsforstyrrelser af forsyningskritiske systemer benyttes desuden til at øge presset på ofre for ransomware-angreb. Vurderingen af truslen fra cyberkriminalitet understøttes af data indsamlet via EnergiCERTs[1] sensornetværk og forekomsten af alvorlige og delvist succesfulde cyberangreb imod danske energivirksomheder i 2021. Begivenheder uden for Danmark bekræfter desuden truslens alvorlighed. I 2021 resulterede ransomware-angrebet på Colonial Pipeline i en alvorlig energikrise i USA, og siden 2015 har den ukrainske energisektor været udsat for flere destruktive cyberangreb. De danske energiselskaber kan altså være sårbare overfor cybertrusler, og de udgør attraktive mål for ondsindede aktører, som ønsker at udnytte digitale sårbarheder.

Sårbarhederne udvikler sig hastigt i takt med, at energisektorerne digitaliseres – en udvikling som drives af den grønne omstilling og implemente-

1 EnergiCERT er en forening ejet af de danske energiselskaber. EnergiCERT'en har udrullet et netværk bestående af 170+ sensorer installeret hos energiselskaber og danner på den baggrund et billede af cybertrusler imod sektoren (Trusselsrapport fra EnergiCERT 2. kvartal 2022).

ringen af smarte digitale løsninger. Udviklingen af digitale sårbarheder hænger sammen med særligt to forhold. For det første er udbredelsen af digitale og internetvendte komponenter og systemer en særlig udfordring for cybersikkerheden i energisektorerne, fordi mange forsyningsprocesser understøttes af operational technology (OT), som ikke altid er designet med fokus på cyber- og informationssikkerhed i samme grad som information technology (IT). For det andet er mange energiselskaber afhængige af leverandører, som selv er afhængige af underleverandører og lange forsyningskæder, hvilket gør dem sårbare over for supply chain-angreb og udbredelsen af sårbarheder i leverandørernes produkter.

Fordi en stabil og pålidelig forsyning af energi udgør grundlaget for samfundets generelle funktionsdygtighed, er den samlede energisektor en samfundskritisk sektor. Derfor påhviler der energisektorernes aktører et særligt ansvar for løbende at tilpasse cyber- og informationssikkerhedsindsatsen, så energiforsyningen ikke påvirkes negativt af truslen fra cyberspace. Da energisektorerne i overvejende grad består af private selskaber, skal dette ansvar løftes i tæt samarbejde mellem den offentlige og den private sektor. Myndighederne skal på den ene side sørge for at stille relevante krav til cyber- og informationssikkerheden i energisektorerne, imens de private energiselskaber på den anden side skal bringe deres viden og kompetencer i spil, så kravene efterleves på en måde som højner cyber- og informationssikkerheden.

Denne strategi er formuleret med udgangspunkt i sektorernes nuværende modenhedsniveau og modstandsdygtighed og med øje for udviklingen i det digitale trusselsbillede for at understøtte, at cybertruslen håndteres ansvarligt.

Strategiens forankring og formål

Denne strategi er en sektorspecifik forlængelse af regeringens nationale strategi for cyber- og informationssikkerhed 2022-2024, som stiller krav om delstrategier for de samfundskritiske sektorer. Strategien følger op på den foregående sektorstrategi for el-, gas- og fjernvarmesektorerne 2019-2021, og viderefører den fælles indsats for at højne cyber- og informationssikkerhed i disse.

Den netop afsluttede strategi var et nybrud i det offentligt-private samarbejde om cyber- og informationssikkerhed på energiområdet, idet el-, gas- og fjernvarmesektorerne gik sammen med myndighederne om at sætte en fælles ambitiøs retning for udviklingen af cyber- og informationssikkerheden. Dette samarbejde har vist sig effektivt og værdiskabende, og fortsættes derfor i den kommende strategiperiode ved videreførelsen af den nuværende styregruppe, som er sammensat af repræsentanter fra Green Power Denmark, Dansk Fjernvarme, Energinet, Klima-, Energi- og Forsyningsministeriet og Energistyrelsen. Implementeringen af de enkelte initiativer vil finde sted i en inklusiv proces, hvor alle relevante aktører inviteres til at bidrage med viden og kompetencer for at sikre strategiens forankring i energisektorerne.

Strategien er desuden resultatet af en omfattende og inddragende proces, hvor energiselskaber, brancheorganisationer, myndigheder og andre interessenter i de tre energisektorer har bidraget til initiativernes indhold. Men strategien er også udarbejdet med blik for de nye fælleseuropæiske krav til cybersikkerhed, som i de kommende år vil blive implementeret i dansk lovgivning i forbindelse med udrulningen af NIS 2.0- og CER-direktiverne[2], samt den nye netværkskode for elnettet og den nationale strategi for cyber- og informationssikkerhed. Et vigtigt formål med strategien er derfor også at forberede energivirksomhederne på de krav, som forventes at følge af implementeringen af disse direktiver i dansk lovgivning. Derudover tager strategien højde for erfaringer og

2 Direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS) og Direktiv om kritiske enheders modstandsdygtighed (CER)

læring fra den foregående strategiperiode, ligesom den bygger videre på det arbejde, som igennem flere år har pågået for at højne cybersikkerheden i energisektorerne, hvor der også er etableret samarbejder på tværs af de samfundskritiske sektorer. Det betyder, at strategien både øger det nuværende ambitionsniveau og sætter ind, hvor der fortsat er behov for en målrettet indsats for at forbedre cyber- og informationssikkerheden og sikre energisektorernes modstandsdygtighed over for de aktuelle trusler.

Det er vigtigt, at energisektorerne også er forberedt på de kommende nye udfordringer, som følger af den grønne omstilling og den ændrede sikkerhedspolitiske situation i Europa. Herunder de udfordringer som cybertruslen skaber for forsyningssikkerheden i takt med den fortsatte digitalisering af samfundet og energisystemerne. Derfor vil de nuværende krav til energiselskabernes cyber- og informationssikkerhed blive opdateret, så Danmark også fremover lever op til internationale krav på området, og er forberedt på at håndtere de udfordringer, som følger med elektrificeringen af samfundet og digitaliseringen af energisystemet. Strategien består derfor af ti konkrete initiativer, som over de næste fire år skal forberede energiselskaberne på at leve op til de kommende lovkrav og dermed løfte cyber- og informationssikkerheden i el-, gas- og fjernvarmesektorerne.

Initiativoversigt

Initiativ 1 Strategisk udvikling af EnergiCERT	**Initiativ 2** OT-sikkerhedsforum
Initiativ 3 Risiko- og sårbarhedsvurderinger	**Initiativ 4** Politikker for cyber- og informationssikkerhed
Initiativ 5 Krisestyring og videreførelse af forretningen	**Initiativ 6** Øvelser
Initiativ 7 Sektorberedskabsforanstaltninger for it-beredskabet	**Initiativ 8** Cybersikkerhed i leverandørforhold
Initiativ 9 Uddannelse, kompetencer og adfærd	**Initiativ 10** Opsamling og operationalisering af viden og data

Initiativ 1

Strategisk udvikling af EnergiCERT

Den markante cybertrussel imod energisektorerne stiller store krav til cyber- og informationssikkerheden i sektorerne og den enkelte energivirksomhed. Disse krav kan, særligt for de mindre virksomheder, være svære at leve op til. Samtidig har sektorerne gavn af en fælles indsats for dataindsamling og videndeling om cybertruslen. Derfor gik el-, gas- og fjernvarmesektorerne sammen om at oprette en sektorCERT[3] i den foregående strategiperiode. EnergiCERT er en forening stiftet og ejet af Energinet, Green Power Denmark og Dansk Fjernvarme. EnergiCERT har siden foreningens stiftelse i 2020 bidraget markant til at løfte energisektorernes cyber- og informationssikkerhed og har i skrivende stund mere end 150 medlemmer blandt energivirksomhederne. Det skyldes, at EnergiCERT samler nogle unikke kompetencer og ressourcer med viden om IT- og OT-sikkerhed i energisystemerne, og anvender dem til gavn for hele sektoren. EnergiCERT arbejder desuden målrettet på at forbedre videndelingen i energisektorerne, hvilket er afgørende for at opnå et højt niveau af cyber- og informationssikkerhed. EnergiCERTs betydning for og bidrag til cyber- og informationssikkerheden i energisektorerne har potentiale til at vokse yderligere i fremtiden og komme alle aktører i energisektorerne til gavn.

I den kommende strategiperiode skal der arbejdes målrettet med EnergiCERTs udvikling. Udviklingen skal tage hensyn til energiselskabernes behov og udviklingen i trusler. Derfor kan EnergiCERTs udvikling tage udgangspunkt i:

- Oprettelse af et OT-observatørkorps. Korpset skal bestå af frivillige eksperter fra energisektorerne, som rykker ud som observatører under cyberhændelser i energisektorerne. Korpset skal indsamle og dele viden om hændelsen med andre energivirksomheder – både under og efter en hændelse

- Udbygning af sensornetværket. EnergiCERT har gennem det seneste år udrullet et omfattende sensornetværk blandt selskaber i energisektorerne. De opsamlede data er med til at løfte cybersikkerheden, da man ikke længere opererer på baggrund af påstande, antagelser og spekulationer. Flere sensorer giver bedre dækning og bedre data, og derfor bør EnergiCERT arbejde på at få så mange selskaber som muligt omfattet af sensornetværket

- Samarbejde på tværs af samfundskritiske sektorer. Det eksisterende samarbejde på tværs af de samfundskritiske sektorer bør understøttes og udvikles, således at angreb mod et selskab i én sektor, deles på tværs af de øvrige sektorer. Samarbejdet eksisterer allerede i dag i regi af samarbejdet imellem de Decentrale Cyber og Informationssikkerhedsenheder (DCIS) og i form af deling af sårbarhedsvarsler. Målrettet arbejde med at strukturere det nuværende samarbejde vil skabe værdi og modstandsdygtighed for selskaberne i energisektorerne og de andre samfundskritiske sektorer. Initiativet støtter på den måde op om den nationale cyber- og informationssikkerhedsstrategi

- Deling af information om trusler. Når en virksomhed udsættes for et cyberangreb, også et mindre betydningsfuldt angreb, kan de i dag dele hændelsen på en tværsektoriel platform for deling af teknisk viden (MISP[4]). Det er langt fra alle selskaber, som i dag er tilsluttet MISP,

3 Computer Emergency Response Team.

4 Malware Information Sharing Platform.

og der bør derfor arbejdes på at øge antallet af aktive brugere. Desuden skal der arbejdes for at uddanne relevante medarbejdere hos energiselskaberne i at anvende platformen, ligesom de data, som deles, i højere grad skal målrettes. Det vil gøre, at hvert selskab får bedre mulighed for at beskytte sig mod igangværende angreb, og at sektorerne samlet set bliver klogere på truslen. Både EnergiCERT, brancheorganisationerne og Energistyrelsen kan spille en rolle i forhold til at øge antallet af tilsluttede brugere på MISP

Initiativ 2

OT-sikkerhedsforum

Den forsyningskritiske teknologi i energisektorerne udgøres primært af operational technology (OT), hvilket adskiller energisektorerne fra de samfundskritiske sektorer i Danmark, hvor IT-systemer i overvejende grad spiller en central rolle i den daglige drift. Mens IT-systemer administrerer data, og dermed regulerer den digitale strøm af information, styrer OT fysiske processer og maskiner i produktionsmiljøer. Skønt IT og OT ikke kan adskilles entydigt, er der altså forskel på, hvad hhv. IT og OT anvendes til, ligesom der er en række forskelle i, hvordan sikkerheden håndteres i de to typer teknologi. Den udbredte anvendelse af OT i energisektorerne skaber derfor nogle særlige forhold omkring cybersikkerhed, som ikke gør sig gældende i IT-dominerede sektorer. Det drejer sig blandt andet om lav indbygget sikkerhed i komponenter og problematikker ift. implementering af cybersikkerhedstiltag i systemer, som ikke er bygget til det. Ydermere er der mangel på ekspertviden og kompetencer i relation til OT-sikkerhed. Derfor skal der oprettes et OT-sikkerhedsforum. OT-sikkerhedsforummet skal bestå af eksperter i OT-sikkerhed på tværs af sektorer, og skal bidrage til udviklingen af cybersikkerheden i energisektorerne. Hvor EnergiCERT bidrager til den daglige sikkerhed i sektorerne gennem dataindsamling, videndeling, uddannelse og vejledning af sine medlemmer, så skal OT-sikkerhedsforummet udgøre et rådgivende og awareness-skabende netværk af eksperter med viden om OT-sikkerhed. Styregruppen inviterer derfor et antal OT-sikkerhedseksperter til at deltage i OT-sikkerhedsforummet. Deltagelsen er frivillig og ulønnet, og det forventes at forummet mødes fire gange årligt. Der skal søges en permanent forankring af forummet i Energistyrelsen, som også varetager sekretariatsfunktionen, således at forummet også fortsætter på den anden side af denne strategis udløb. Forummet skal blandt andet:

- Rådgive styregruppen for sektorstrategien, myndigheder og selskaber i energisektorerne om OT-sikkerhed
- Skabe opmærksomhed om cyber- og informationssikkerhed blandt ledelser og bestyrelser i energiselskaber
- Sætte dagsordenen i relation til OT-sikkerhed i både sektorerne og nationalt. For eksempel ved at udpege OT-sikkerhedsrelaterede emner, som energiselskaberne bør have særligt fokus på
- Indgå i dialog med leverandører af OT til energisektorerne
- Udfærdige lister over produkter og leverandører med høj grad af IT- og OT-sikkerhed i deres løsninger
- Bygge bro på tværs af de samfundskritiske sektorer som benytter OT

Initiativ 3

Risiko- og sårbarhedsvurderinger

Vurderinger af risici og sårbarheder er grundlaget for, at hvert energiselskab kan arbejde risikobaseret med cyber- og informationssikkerhed. Ved at inddrage viden om det aktuelle trusselsbillede sætter risiko- og sårbarhedsvurderinger energiselskaber i stand til at prioritere og målrette deres indsatser der, hvor det giver mest værdi og størst sikkerhed. Det er desuden et lovkrav, at bevillingspligtige virksomheder i el- og naturgassektorerne foretager risiko- og sårbarhedsvurderinger, og anvender resultaterne af disse som grundlag for deres arbejde med IT-beredskab og cybersikkerhed.

Det kommende NIS 2.0-direktiv stiller også skarpt på en risikobaseret tilgang. Energistyrelsen har i en årrække udarbejdet risikoscenarier til energiselskaberne, som skal bidrage til deres risiko- og sårbarhedsanalyser. I 2021 var der 45 beskrevne scenarier, hvoraf ca. 20 direkte omhandlede cybertrusler. For at sikre at virksomhederne får det fulde udbytte af risikoscenarierne, og desuden er i stand til at udarbejde værdiskabende risiko- og sårbarhedsanalyser i relation til alle dele af deres forretning, er det nødvendigt med en indsats som udvikler deres kompetencer. Dette gør sig gældende for el- og gasselskaber, som er forpligtede til at basere deres arbejde med cyber- og informationssikkerhed på risiko- og sårbarhedsvurderinger, men det er særligt vigtigt at kompetencerne udbredes til fjernvarmesektoren, som ikke er underlagt krav herom endnu.

Derfor skal der i den kommende strategiperiode arbejdes med at højne særligt de mindre energiselskabers kompetencer ift. at foretage anvendelige og værdiskabende risiko- og sårbarhedsvurderinger. Arbejdet skal identificere og kommunikere good practice på området samt formidle dette til IT-beredskabsansvarlige og ledelser i energisektorerne. Arbejdet med risiko- og sårbarhedsvurderinger kan tage udgangspunkt i:

- Hensyn til nuværende og forventede lovkrav
- Udarbejdelse af metoder til risiko- og sårbarhedsvurderinger af eksempelvis IT- og OT-systemer, komponenter og services
- Udarbejdelse af good practice for procedurer for logning, backuppolitikker, sikkerhedskopiering mv.
- Videreudvikling af Energistyrelsens IT-ROS-scenarier og hvordan værdien af disse kan øges på tværs af sektorer og selskaber
- Opmærksomhedsskabende indsatser, som kommunikerer værdien af risiko- og sårbarhedsanalyser EnergiCERT'en bør inddrages i arbejdet mhp. at koordinere eventuelle parallelle indsatser og afsøge muligheden for at der oprettes et online kursus i risiko- og sårbarhedsvurdering i regi af EnergiCERT

Desuden kan muligheden for at lave en indsats, som målrettes de større selskaber, afsøges. En sådan indsats skal tage hensyn til, at de større energiselskaber – særligt i el- og gassektorerne – har andre forudsætninger for udarbejdelsen af risiko- og sårbarhedsvurderinger, herunder anvendelsen af IT-ROS-scenarier.

Den digitale trussel imod energisektorerne er meget høj, hvilket har vist sig ved flere cyberangreb på energiselskaber

Initiativ 4

Politikker for cyber- og informationssikkerhed

Virksomhedspolitikker medvirker til, at beslutninger udmøntes i konkrete handlinger. Men de udgør også værktøjer, som kan hjælpe virksomheder med at træffe gode og reflekterede beslutninger om interne arbejds- og forretningsprocesser. Dette gør sig også gældende i forhold til cybersikkerhed, hvor ledelsesgodkendte politikker giver medarbejdere mandat til at implementere sikkerhedsoptimerende tiltag.

Der vil i de kommende år blive stillet mere omfattende krav i form af bl.a. lovgivning til energiselskabers virksomhedspolitikker på cybersikkerhedsområdet. Det er derfor vigtigt, at selskaberne er i stand til at udforme politikker, som er anvendelige og værdiskabende for deres arbejde med cybersikkerhed. F.eks. i forhold til logning, hvor hver enkelt virksomhed med udgangspunkt i en risiko- og sårbarhedsvurdering bør formulere en politik, som tager stilling til, hvor meget data der logges, hvordan det behandles og i hvor lang tid det opbevares – og meget mere. Derfor skal der i den kommende strategiperiode arbejdes med udviklingen af good practice for virksomhedspolitikker inden for cyber- og informationssikkerhed. Arbejdet kan tage udgangspunkt i følgende:

- Der udarbejdes good practice og/eller metoder for udarbejdelse af virksomhedspolitikker for logning, backup, asset-management, medarbejderadfærd og leverandørsikkerhed, herunder med særligt fokus på en holistisk tilgang til sammenhængen mellem politikkerne
  - Metoderne for udarbejdelse af politikker skal tage højde for anvendelsen af risiko- og sårbarhedsvurderinger, good practice, internationale standarder samt vejledninger fra f.eks. CFCS, Energistyrelsen og andre myndigheder
- Arbejdet skal harmoniseres med nuværende og forventede lovkrav

Initiativ 5

Krisestyring og videreførelse af forretningen

Den digitale trussel imod energisektorerne er meget høj, hvilket har vist sig ved flere cyberangreb på energiselskaber. Energivirksomheder må derfor, og det på trods af deres arbejde med cybersikkerhed, forvente at blive ramt af cyberangreb. Som energiselskab er det naturligvis vigtigt, at man implementerer relevante tiltag for at forebygge cyberangreb, men det er mindst

ligeså vigtigt, at man ruster sig til at fortsætte driften af forsyningskritiske processer under en cyberhændelse. Det er blandt andet derfor, at der er lovkrav om beredskabsplaner med beskrivelser af procedurer for etablering af alternativ drift ved nedbrud på forsyningskritiske it-systemer og planer for genopretning af disse. For at støtte op om selskabernes evner til at efterleve kravene om fortsat drift under et cyberangreb sættes der øget fokus på forberedelse af krisestyring og videreførelse af både forretningen og de forsyningskritiske processer under en cyberhændelse.

Derfor skal der i den kommende strategiperiode arbejdes med at forbedre kvaliteten af energivirksomhedernes planer for business continuity og krisestyring. Arbejdet kan tage udgangspunkt i:

- Udarbejdelse af en branchestandard for krisestyring baseret på good practice i energisektorerne
- Udarbejdelse af en branchestandard for business continuity baseret på good practice i energisektorerne
- Temadage med fokus på krisestyring, beredskabsplanlægning og business continuity
- Arbejdet bør inddrage nuværende og forventede lovkrav

Initiativ 6

Øvelser

Ved at afholde øvelser og gennemføre øvelsesevalueringer kan virksomheder og myndigheder sikre sig, at de planer og procedurer for krisestyring og videreførelse af forretningen, som er udviklet til at håndtere cybersikkerhedshændelser, faktisk efterleves. Øvelser tjener til at kontrollere, at de involverede parter kender deres roller og ansvar, men det er også en værdifuld måde at lære på – uden at det har konsekvenser for forsyningssikkerheden. Øvelser er også en mulighed for præventivt at afdække roller, ansvar og kommunikationsveje under hændelser. Den nationale strategi for cyber- og informationssikkerhed stiller krav om, at der gennemføres årlige sektorspecifikke cyberberedskabsøvelser i de samfundskritiske sektorer. Derudover er det et krav, at DCISerne skal have en operativ kapacitet, som kan sættes ind under cyberhændelser. Denne kapacitet kan testes og optimeres gennem deltagelse i sådanne øvelser. Øvelserne kan desuden træne samarbejdet mellem DCIS-Energi og andre DCISer, Energinet, EnergiCERT, CFCS og andre energisektorer under hændelser.

Afholdelse af øvelser er selskabernes og myndighedernes mulighed for at lære at håndtere kriser, før de rammer. Derfor er det vigtigt, at energisektorerne afholder relevante øvelser både inden for de enkelte virksomheder med inddragelse af it-sikkerhedstjenester, i de enkelte sektorer, på tværs af energisektorerne, men i særdeleshed også på tværs af de samfundskritiske sektorer som efterspurgt i DCIS-kredsen. Samtidigt er det vigtigt, at disse øvelser ikke begrænser sig til simulationer, men også inddrager fysiske elementer.

Derfor skal der i den kommende strategiperiode arbejdes med, at øvelser bliver en integreret del af alle energiaktørers arbejde for øget cybersikkerhed. Med det formål skal der:

- Arbejdes med at højne energiselskabernes forståelse for vigtigheden af at afholde cyberberedskabsøvelser

- Skabes de nødvendige forudsætninger for, at flere energiselskaber afholder relevante og værdiskabende øvelser inden for egen organisation

- Afholdes cyberberedskabsøvelser i de enkelte energisektorer

- Afholdes årlige cyberberedskabsøvelser på tværs af energisektorerne

- Deltages aktivt i arbejdet med afholdelse af cyberberedskabsøvelser på tværs af flere og gensidigt afhængige samfundskritiske sektorer

Initiativ 7

Sektorberedskabsforanstaltninger for it-beredskabet

En del af energisektorernes samlede beredskab beror på, at Energinet i krisesituationer kan iværksætte tværgående sektorberedskabsforanstaltninger[5]. Sektorberedskabsforanstaltningerne består af instrukser til energiselskaberne om, hvad de konkret skal gøre for at hæve beredskabet. Der findes i dag 29 klassiske/fysiske sektorberedskabsforanstaltninger for el- og gassektoren, der kan aktiveres under en sikkerhedshændelse, eksempelvis øget tilsyn med bygninger og kontrol med adgang til anlæg. Udarbejdelsen af disse foranstaltninger har bidraget til større klarhed over handlemuligheder og forventninger til energiselskaberne under hændelser.

Der findes i dag ikke tilsvarende foranstaltninger for cyberhændelser, men i lyset af forskelle i modenhedsniveauer og kompetencer på tværs af energisektorerne, er det imidlertid nødvendigt med en fælles og tværgående forståelse for tilgangen til håndteringen af cyberhændelser. Sektorberedskabsforanstaltninger bidrager nemlig til, at sektorerne reagerer ensartet på tværgående trusler, og derigennem afhjælper de, at mindre virksomheder med færre kompetencer og ressourcer bliver en mulig angrebsflade og dermed udgør en risiko for resten af sektoren.

Derfor skal der i den kommende strategiperiode arbejdes med at formulere sektorberedskabsforanstaltninger på cyberområdet, som kan styrke energisektorernes evne til at håndtere cyberhændelser. Arbejdet kan tage udgangspunkt i:

- Udvikling af en fælles forståelse for beredskabsniveauer ved en cyberhændelse

- Udarbejdelse af cyberberedskabsforanstaltninger, som kan anvendes på tværs af energisektorerne

5 Tværgående foranstaltninger som iværksættes med henblik på at imødegå konsekvenser af en beredskabshændelse.

Initiativ 8

Cybersikkerhed i leverandørforhold

Leverandørsikkerhed indgik også som et initiativ under den seneste strategi for cyber- og informationssikkerhed i energisektorerne (2019-2021). Emnet bliver kun vigtigere i takt med, at flere energivirksomheder anvender leverandører til flere områder af deres forretning, og flere prominente leverandører bliver mål for cyberangreb. Samtidig med at sektorerne bliver mere afhængige af eksterne leverandører i driften af deres forretning, bliver leverandørerne større og mere komplekse. Derfor er det vigtigt, at energiselskaber har fokus på cybersikkerheden i leverandørforhold. Anvendelsen af leverandører kan medvirke til øget cybersikkerhed, hvis leverandøren er kompetent og virksomheden vil betale, hvad sikkerheden koster. Men leverandørforhold kan også være en kilde til brud på cybersikkerheden. F.eks. kan virksomhedens cybersikkerhedsniveau falde, hvis cybersikkerhed ikke er indtænkt i den pågældende leverance, og leverandører med lav cybersikkerhed kan blive en angrebsvej ind i virksomheden, som angribere eller andre aktører udnytter.

Derfor skal der i den kommende strategiperiode arbejdes målrettet med at højne cybersikkerheden i leverancer til energisektorerne. Dette arbejde kan blandt andet tage udgangspunkt i:

- Udvikling af en branchestandard for energiselskabers samarbejde med leverandører om beredskabsplanlægning og øvelser

- Den seneste strategis initiativ 3 og 7, hvor der arbejdes videre med leverandørsikkerhed i relation til IT, OT og IIoT (Industrial Internet of Things). F.eks. ved udarbejdelse af en vejledning til de mindste energivirksomheder, som sætter dem i stand til at udvikle simple kravkataloger til leverandører af IIoT baseret på risiko- og sårbarhedsvurderinger og egne politikker

- Udarbejdelse af tekniske forskrifter for brug af IoT- og IIoT udstyr, herunder arbejde med sikkerheden i produkter med betydning for energisektorerne, så som ladestandere, varmepumper o. lign.

- Involvere CFCS i udfærdigelsen af cybersikkerhedskrav i forbindelse med indkøb og udbud af samfundskritiske IT-systemer i energisektorerne

- Styregruppen kan foranstalte en dialog mellem relevante myndigheder (Energistyrelsen, CFCS, Digitaliseringsstyrelsen etc.), OT-sikkerhedsforummet, andre relevante interessenter og relevante leverandører til energisektorerne

  - Dialogen kan omhandle cybersikkerhed i leverancer, leverandørsikkerhed og hvilken rolle leverandører spiller både i daglig drift og under kriser og hændelser i energisektorerne

Initiativ 9

Uddannelse, kompetencer og adfærd

Viden om cybersikkerhed på alle niveauer er helt central, hvis en virksomhed skal opnå et tilstrækkeligt modenheds- og modstandsdygtighedsniveau. Der er mange kompetente IT-sikkerhedsmedarbejdere i energivirksomhederne, men det er ikke tilstrækkeligt, at specialisterne er klædt på til at løse deres opgave. Det er også vigtigt, at beslutningstagerne, som definerer rammerne for opgaveløsningen, nemlig bestyrelser og direktioner, har tilstrækkelig viden til at træffe gode og rigtige beslutninger, når det drejer sig om cybersikkerhed. I relation hertil forventes det, at NIS 2.0 vil stille krav om, at direktioner i energivirksomheder jævnligt modtager relevant uddannelse i cybersikkerhed og desuden står til ansvar for beslutninger vedrørende cyber- og informationssikkerhed.

En anden risiko ligger i, at de fleste arbejdsgange i dag er digitaliserede. Det kan øge antallet af potentielle sårbarheder i den enkelte virksomheds forsvar. Derfor er det vigtigt, at cybersikkerhed tænkes ind på alle niveauer af virksomhedernes forretning. Angribere vil typisk forsøge at få adgang til systemerne gennem steder i organisationen, hvor angreb ikke forventes, og derfor kan selv den administrerende direktørs eller receptionistens digitale adfærd være en vigtig brik til øget cybersikkerhed.

Selvom der er mange dygtige IT-specialister i energisektorerne, så er det nødvendigt, at der konstant arbejdes på at øge tilgangen af IT- og OT-specifikke kompetencer og ressourcer til energisektorerne. Uddannelse af kompetente medarbejdere til energiselskaberne er den vigtigste forsikring for, at energisektorerne også i fremtiden kan levere en høj og stabil forsyningssikkerhed.

Derfor skal energisektorerne i den kommende strategiperiode arbejde målrettet med at hæve uddannelsesniveauet i relation til cybersikkerhed og påvirke medarbejdere og lederes digitale adfærd og beslutningstagning i en positiv retning. Derudover skal der arbejdes for, at der i fremtiden er flere OT- og IT-sikkerhedskompetencer til rådighed, som kan bidrage til cybersikkerheden i energisektorerne. Arbejdet kan tage udgangspunkt i:

- Udvikling af en vejledning til, hvordan energivirksomheder kan arbejde seriøst, risikobaseret og kontinuerligt med at skabe sikker digital medarbejderadfærd

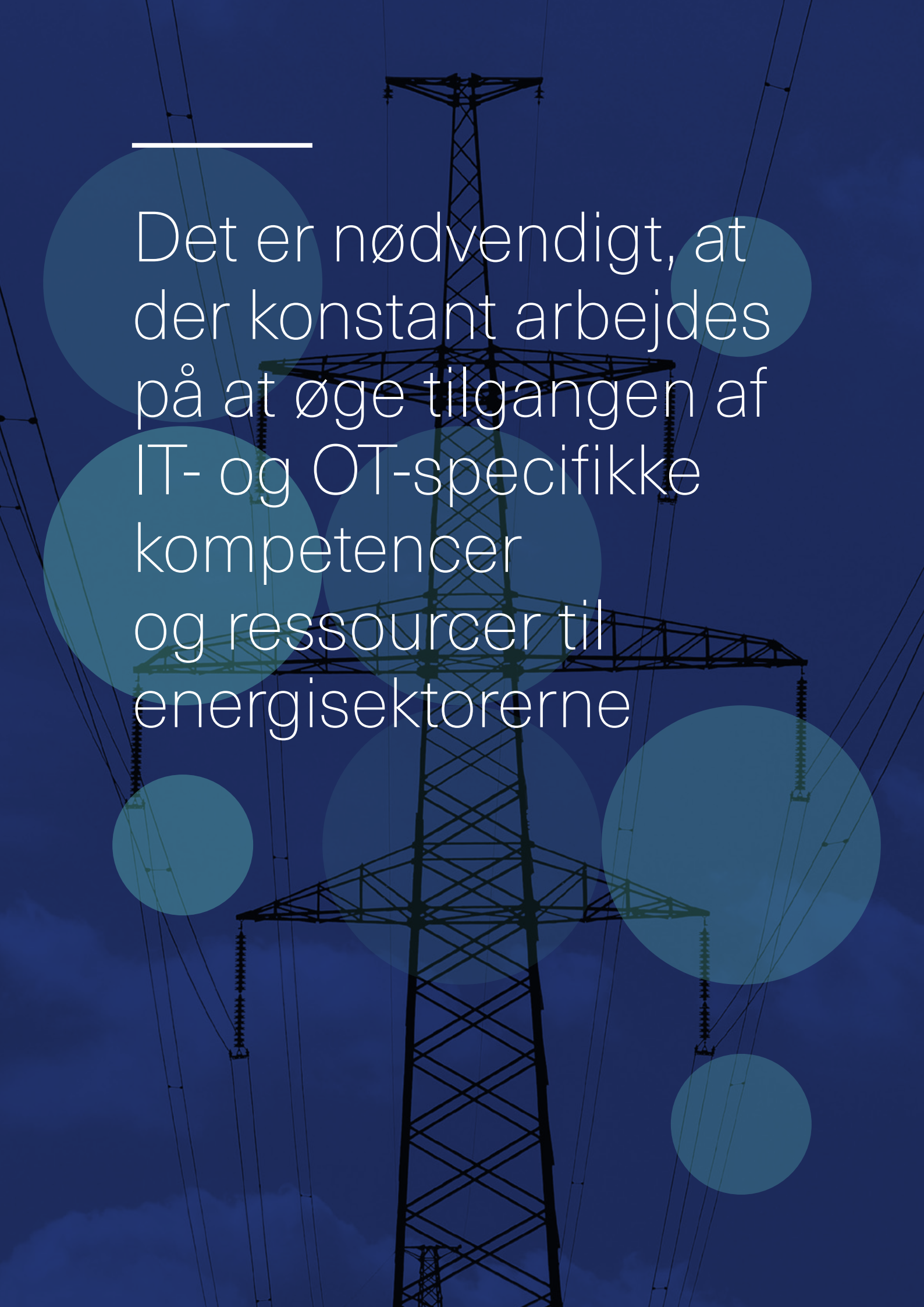
- Afsøge mulighederne for, at der udbydes uddannelse i cybersikkerhed målrettet ledelser og bestyrelser, samt uddannelse og træning af IT-beredskabsansvarlige

- Arbejdet bør inddrage EnergiCERT med henblik på at afsøge mulighederne for at oprette et online kursus i sikker digital og fysisk medarbejderadfærd, samt opsamle erfaringer med de nuværende kurser, som EnergiCERT udbyder

- EnergiCERT udarbejder et uddannelsesforløb i cybersikkerhed målrettet ledelser og bestyrelser
  - OT-sikkerhedsforummet kan rådgive EnergiCERT i arbejdet med at udarbejde et uddannelsesforløb

- OT-sikkerhedsforummet inviterer relevante uddannelsesinstitutioner til dialog om oprettelse af flere OT-sikkerhedskompetencegivende uddannelser

- Energistyrelsen faciliterer, i samarbejde med andre sektoransvarlige myndigheder, styregruppen og OT-sikkerhedsforummet, en dialog med relevante uddannelsesinstitutioner for at øge udbuddet af relevante uddannelser



Det er nødvendigt, at der konstant arbejdes på at øge tilgangen af IT- og OT-specifikke kompetencer og ressourcer til energisektorerne

Initiativ 10

Opsamling og operationalisering af viden og data

Arbejdet med at højne cybersikkerheden i energisektorerne genererer en stor mængde viden og data. Både Energistyrelsen, EnergiCERT og Energinet indsamler løbende viden og data om cybersikkerheden i energisektorerne gennem tilsyn, hændelsesindberetninger, sensorer, rådgivning, og andre aktiviteter. Der er altså et stort uudnyttet potentiale for, gennem målrettet arbejde med disse videns- og datakilder, at generere yderligere sektorspecifik viden, som kan bruges til at målrette og udvikle arbejdet med cyber- og informationssikkerhed.

Derfor skal der i den kommende strategiperiode arbejdes målrettet med at samle op på denne viden og operationalisere den til konkrete og værdiskabende tiltag. Arbejdet kan tage udgangspunkt i:

- En kortlægning af tilgængelig viden og data om cybersikkerhed i energisektorerne
- Drøftelse af den konkrete håndtering af denne viden, og hvordan den kan indsamles og opbevares
- Udforskning af mulighederne for at operationalisere denne gennem forskning, løbende anvendelse o. lign. med henblik på at højne resiliensen i sektoren

Årlig revision og justering

Cybersikkerhed er et område i rivende udvikling. Denne udvikling hænger sammen med den konstante udvikling i cybertruslerne, men drives også af den fortsatte digitalisering, som skaber nye sårbarheder og ændrer konsekvenserne af hændelser i takt med stigningen i digitale sammenkoblinger.

For at sikre strategiens fortsatte relevans vil styregruppen én gang årligt revidere det strategiske arbejde, se fremad og forholde sig til nye tiltag og den cybersikkerhedsmæssige udvikling i energisektorerne. På baggrund heraf vil strategien blive tilpasset, udviklet eller videreført uændret.

Som en del af den årlige revision beslutter styregruppen i samarbejde med OT-sikkerhedsforummet og EnergiCERT et tema, der skal arbejdes med i løbet af det kommende år. EnergiCERT og OT-sikkerhedsforummet driver i samarbejde denne dagsorden og arbejder for at operationalisere temaet til konkrete initiativer, som energiselskaberne kan arbejde med. Formålet er at understøtte og drive en konstant udvikling af cybersikkerheden i energisektorerne.

September 2022

Design: GEUS
Fotos: Colourbox
Publikationen kan hentes på
www.ens.dk/publikationer

Energistyrelsen
Carsten Niebuhrs Gade 43
1577 København V

Telefon: 33 92 67 00
E-mail: dcis-energi@ens.dk
www.ens.dk