Miljøministeriet
Miljøstyrelsen

Strategi for cyber- og informations-sikkerhed i vandsektoren 2023-2025

Orientering fra
Miljøstyrelsen nr.58

December 2022

Udgiver: Miljøstyrelsen

Redaktion: Miljøstyrelsen

Indhold

1.	**Forord**	**4**
2.	**Indledning**	**5**
3.	**Afgrænsning**	**6**
3.1	Introduktion til vandsektoren	6
3.2	Definition af cyber- og informationssikkerhed	6
3.3	Kritisk infrastruktur i vandsektoren	6
3.4	Kritisk it-infrastruktur i vandsektoren	7
4.	**Trusler, risici og sårbarheder**	**8**
4.1	Nøgleobservationer om cyber- og informationssikkerheden i vandsektoren	8
4.2	Vurdering af cyber- og informationssikkerhedstruslen mod vandsektoren	9
5.	**Styrket indsats for cyber- og informationssikkerheden i vandsektoren**	**10**
5.1	Miljøstyrelsens cyber- og informationssikkerhedsenhed	10
5.1.1	Initiativ 1: It-sikkerhedspolitik	12
5.1.2	Initiativ 2: It-beredskabsplan	13
5.1.3	Initiativ 3: Styrket samarbejde mellem Miljøstyrelsen og vandsektoren	14
5.1.4	Initiativ 4: Koordinering med EnergiCERT	14
5.1.5	Initiativ 5: Yderligere kortlægning af kritisk it-infrastruktur	15
5.1.6	Initiativ 6: Anbefalinger til vandsektoren om konkrete tiltag	16
5.2	Implementering af EU-lovgivning	16
6.	**Arbejdsprogram**	**18**
6.1	Tidshorisont	18
7.	**Årlig revision og revidering**	**19**
7.1	Årlig revision og revidering	19

1. Forord

”National strategi for cyber- og informationssikkerhed 2022-2024” fra december 2021 har til formål at skabe en robust beskyttelse af vores samfundsvigtige funktioner. En robust vandsektor er en grundsøjle i vores samfund. Borgere og virksomheder er i det daglige helt afhængige af at kunne få drikkevand. Samtidig er håndteringen af spildevand fra huse og industri afgørende for at vores samfund kan fungere.
Samfundsvigtige funktioner er fx vandværker, rensningsanlæg og ledningsnet.

Vi lever i en tid, hvor vandforsyning ikke kun afhænger af vandværker, rensningsanlæg og ledningsnet. Digitalisering er en afgørende drivkraft for udviklingen af vores samfund, og det gælder også vandsektoren. Styringen af drikkevand- og spildevand er mange steder koblet til it-systermer. Med den øgede grad af digitalisering følger også en øget sårbarhed over for cyberangreb.

Der er ikke tale om en teoretisk problemstilling. Tværtimod har der desværre allerede været flere eksempler på cyberangreb mod forsyninger i Danmark. Vi skal sikre, at den øgede grad af digitalisering ikke bliver på bekostning af forsyningssikkerheden. Cybersikkerhed er også forsyningssikkerhed.

Den danske vandsektor brænder for den grønne omstilling og for at sætte forsyningssikkerheden i højsæde. Det er afgørende for trygheden og tilliden til forsyningsområdet for drikkevand og spildevand, at vandsektoren også er robust over for cyberangreb.

Vi er glade for at kunne lancere Miljøstyrelsens ”Strategi for cyber- og informationssikkerhed i vandsektoren 2023-2025”. Strategien indeholder en række konkrete og vigtige initiativer for forsyningsområdet for drikkevand og spildevand i Danmark. Strategien udgør stærk en ramme for de kommende års arbejde med at understøtte og styrke cyber- og informationssikkerheden i den danske vandsektor.

Vicedirektør Lars Møller Christiansen og vicedirektør Isabelle Navarro Vinten, Miljøstyrelsen, december 2022

2. Indledning

Regeringen lancerede den 15. december 2021 en ny "National strategi for cyber- og informationssikkerhed 2022-2024" for at styrke indsatsen over for digitale trusler. Som led i udmøntningen af den nationale strategi har Miljøstyrelsen udarbejdet en strategi for cyber- og informationssikkerhed i vandsektoren i samarbejde med interessenter fra den danske vandsektor.

Den nationale strategi for cyber- og informationssikkerhed har fire strategiske målsætninger, der til sammen sætter rammen for udviklingen mod et stærkere og mere sikkert digitalt Danmark:

- "1. Robust beskyttelse af samfundsvigtige funktioner",
- "2. Øget kompetenceniveau og ledelsesforankring",
- "3. Styrkelse af det offentligt-private samarbejde"
- "4. Aktiv deltagelse i den internationale kamp mod cybertruslen".

Med regeringens strategi sættes der nationalt krav om, at der formuleres delstrategier for arbejdet med cyber- og informationssikkerhed i de samfundsvigtige sektorer. Nærværende strategi er delstrategien for cyber- og informationssikkerhed i vandsektoren. Drikkevand og spildevand er blevet defineret som samfundsvigtige funktioner og dele af vandsektorens infrastruktur betragtes som kritisk infrastruktur. Nærværende strategi sætter rammerne for Miljøstyrelsens og den samlede vandsektors arbejde med at realisere den nationale cyber- og informationssikkerhedsstrategi i forhold til at forbedre cyber- og informationssikkerheden på tværs af vandsektoren.

Arbejdet med cyber- og informationssikkerhed er baseret på det såkaldte sektoransvarsprincip, hvor de enkelte ressortministerier har ansvar for de sektorer, der hører under deres område. Sektoransvaret for vandsektoren ligger hos Miljøstyrelsen. Ansvaret omfatter bl.a. at Miljøstyrelsen kortlægger den kritiske it-infrastruktur i vandsektoren, udarbejder en strategi for vandsektoren og opretter en såkaldt decentral cyber- og informationssikkerhedsenhed (DCIS) på området.

3. Afgrænsning

Strategien for cyber- og informationssikkerhed fokuserer primært på den kritiske it-infrastruktur i vandsektoren. Det er nødvendigt at tage højde for, at der er store forskelle imellem vandselskaberne på tværs af vandsektoren.

3.1 Introduktion til vandsektoren

Vandsektoren er en samlet betegnelse for de vandselskaber, der forsyner danskerne med drikkevand og renser og transporterer spildevand. Vandsektoren er decentraliseret og består i dag af ca. 2.500 almene drikkevandsselskaber og ca. 100 spildevandsselskaber. Hovedparten af de almene drikkevandsselskaber er mindre, forbrugerejede vandværker og en mindre andel er kommunalt ejede. De kommunalt ejede vandforsyningsselskaber står for ca. to tredjedele af den samlede produktion af drikkevand. Spildevandsselskaberne er primært kommunalt ejede.

På drikkevandsområdet findes der store multiforsyningsselskaber, der producerer adskillige millioner kubikmeter vand om året. Samtidig findes der også små almene vandværker, der forsyner helt ned til 10 ejendomme med drikkevand. Herudover er der en underskov af primært små private vandforsyninger, der forsyner under 10 ejendomme. På spildevandsområdet er der ca. 100 kommunalt ejede spildevandsselskaber – ét selskab pr. kommune – der varetager ca. 700 ud af ca. 850 renseanlæg i Danmark.

Miljøstyrelsens strategi vedrører cyber- og informationssikkerheden for de almene vandforsyninger og de kommunalt ejede spildevandsanlæg, og strategien fokuserer primært på vandsektorens kritiske it-infrastruktur. Det vil blive behandlet nærmere i dette kapitel, hvordan vandsektorens kritiske it-infrastruktur skal forstås. Derudover er der et selvstændigt initiativ i strategien, der vil foretage yderligere kortlægning af den kritiske it-infrastruktur i vandsektoren, jf. strategiens initiativ 5 ”Yderligere kortlægning af kritisk it-infrastruktur”.

3.2 Definition af cyber- og informationssikkerhed

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

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 bl.a. med organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikkerhedsforanstaltninger.

3.3 Kritisk infrastruktur i vandsektoren

Forsvarsministeriet har givet retningslinjer for, hvornår infrastruktur er kritisk infrastruktur. Kritisk infrastruktur er infrastruktur, der påvirker samfundets generelle funktionsdygtighed, og hvor der er få eller ingen substitutionsmuligheder, samtidig med at infrastrukturen anvendes i bredt omfang. Samfundets generelle funktionsdygtighed påvirkes, hvis et nedbrud eller beskadigelse af infrastrukturen i mindre end 7 dage resulterer i en alvorlig krise i samfundet med mindst én af følgende konsekvenser:

a) Alvorligt antal døde, alvorligt sårede eller kronisk syge,
b) Alvorlige samfundsøkonomiske konsekvenser,
c) Alvorligt antal personer med fysiske eller psykiske lidelser,
d) Alvorlig reduktion i tilliden til staten, offentlige institutioner eller borgernes generelle tryghedsfølelse,
e) Nedbrud af anden kritisk infrastruktur. Endvidere er der også tale om kritisk infrastruktur såfremt infrastrukturen er meget vigtig for, at en krise der allerede er opstået kan håndteres, så negative skadevirkninger bliver begrænset.

På baggrund af ovenstående operationalisering har Mijløstyrelsen – i samarbejde med Deloitte – vurderet, at den kritiske infrastruktur er alle multiforsyningsselskaber, alle store vandforsyningsselskaber samt alle kommunale spildevandsselskaber. For disse selskaber er det fx deres boringer, brønde, pumpestationer, distributionsnet og renseanlæg der er kritisk infrastruktur. Ved multiforsyningsselskaber forstås selskaber med over 800.000 m^3 producerede vandmængder årligt og yderligere forsyningsarter, og ved store selskaber forstås selskaber med over 800.000 m^3 producerede vandmængder årligt. Til sammen udgør disse selskaber ca. 65 % af den samlede behandlede vandmængde og dækker samtidig et stort geografisk område. De fungerer endvidere i høj grad som nødforsyning for de mindre selskaber og forsyner desuden i vid udstrækning øvrige kritiske funktioner som fx sundhedsvæsenet. Samtlige kommunale spildevandselskaber bør omfattes, fordi der ikke er reelle substitutionsmuligheder på spildevandsområdet.

3.4 Kritisk it-infrastruktur i vandsektoren

Miljøstyrelsen har valgt at definere den kritiske it-infrastruktur i vandsektoren som de systemer, der er nødvendige for at opretholde eller genoprette forsyningen af drikkevand og afledningen af spildevand hos de selskaber, der er en del af den kritiske infrastruktur. For at kunne afdække systemunderstøttelsen af vandselskabernes produktion er det nødvendigt at fokusere på vandselskabernes såkaldte ”Operationelle Teknologi” (OT), som er en samlet betegnelse for den software og hardware, der styrer, overvåger og kontrollerer det industrielle produktionsapparat, dvs. drikkevandsproduktion, drikkevandsdistribution, spildevandstransport og spildevandsbehandling.

Den kritiske it-infrastruktur skal findes hos de vandselskaber, der på baggrund af udvælgelseskriterierne er omfattet af den kritiske infrastruktur. For disse selskaber gælder det, at den kritiske it-infrastruktur er defineret som den digitale infrastruktur, der er nødvendig for opretholde produktionen og distribueringen af drikkevand samt indsamling, rensning og afledning af spildevand. Dette gælder primært selskabernes OT-systemer. Eksempler på OT-systemer er SRO-anlæg, SCADA og PLC’er.

Tilgangen med at kortlægge den kritiske it-infrastruktur med udgangspunkt i vandsektorens kritiske infrastruktur er udtryk for en pragmatisk tilgang til, hvad der har været muligt. Der kan således godt være it-systemer, der anvendes af flere drikkevands- og spildevandsselskaber og derfor er tilkoblet til OT-systemer, der til sammen leverer en volumen på over 800.000 m^3.

Det er afgørende at definitionen og kortlægningen af kritisk it-infrastruktur er i overenstemmelse med det kommende NIS2-direktiv, se nærmere herom under afsnittet ” Initiativ 5: Yderligere kortlægning af kritisk it-infrastruktur”

4. Trusler, risici og sårbarheder

I dette afsnit gives en vurdering af trusler, risici og sårbarheder i vandsektoren for så vidt angår cyber- og informationssikkerhed.

Strategiens trusselsvurdering er baseret på Center for Cybersikkerheds (CFCS) trusselsvurdering for energisektoren fra juli 2022 og EnergiCERT's trusselsvurdering for energisektoren fra oktober 2022. Der er ikke hidtil blevet udarbejdet selvstændige trusselvurderinger for vandsektoren, men i 2023 vil EnergiCERT's trusselsvurderinger også omfatte vandsektoren.

Der er i forbindelse med forarbejdet til denne strategi foretaget en dataindsamling med henblik på at tegne et selvstændigt billede af cyber- og informationssikkerheden i vandsektoren. Data er indsamlet af Deloitte på vegne af Miljøstyrelsen via inputs fra workshops og en spørgeskemaundersøgelse, der er blevet udsendt til et repræsentativt udsnit af vandsektorens forsyningsselskaber.

4.1 Nøgleobservationer om cyber- og informationssikkerheden i vandsektoren

Nedenstående figur viser de nøgleobservationer, der er blevet fundet i undersøgelsen af cyber- og informationssikkerheden i vandsektoren. Observationerne er både af positiv og negativ karakter og benyttes ikke kun til at fremhæve områder, hvor vandsektoren kan styrke cyber- og informationssikkerhed, men også områder hvor vandsektoren står stærkt. Nøgleobservationerne er med til at danne baggrund for valget af de tiltag, der indgår i denne strategi.

Observation	Beskrivelse
1	Det generelle niveau for cybersikkerhed i vandsektoren vurderes til at være over middel, men falder relativt med selskabernes størrelse (faldende).
2	Adskillelse af IT- og OT-systemer er essentielt for at sikre forsyningssikkerheden.
3	En signifikant andel af vandsektoren har ikke tegnet en cyberforsikring.
4	It-sikkerhed og hændelseshåndtering outsources til eksterne partnere på tværs af vandsektoren.
5	Forsyningssikkerheden er i høj grad afhængig af evnen til at kunne køre manuel drift af anlægget i tilfælde af hændelser. En betydelig andel af vandselskaber tester ikke eller kun delvist evnen til at kunne køre manuel drift.
6	Vandselskaberne har fokus på uddannelse og awareness, men andelen, der uddanner deres medarbejdere, falder i takt med vandselskabets størrelse.
7	Der er behov for standardisering af vandsektorens it-infrastruktur, hvis cyberniveauet skal løftes på tværs af sektoren.
8	Små og mikro-vandselskaber har enten ikke eller kun delvist en dokumenteret it-sikkerhedspolitik.
9	Multiforsyningsselskaber fokuserer primært på cyber- og informationssikkerhed, der omfatter anden kritisk infrastruktur de er ansvarlige for (fx energi).

4.2 Vurdering af cyber- og informationssikkerhedstruslen mod vandsektoren

CFCS vurderer, at truslen for cyberspionage mod energisektoren er meget høj. Derudover vurderer CFCS, at truslen især er rettet mod produktions- og transmissionsselskaber i energisektoren. CFCS vurderer også, at truslen for cyberkriminalitet er meget høj. Begrebet cyberkriminalitet defineres som tilfælde, hvor personer og eller et netværk udfører cyberangreb, hvor formålet er berigelse. Angreb med det formål at låse administrative it-netværk og it-infrastruktur kan ifølge CFCS i værste fald true forsyningssikkerheden. Det kan fx ske som en konsekvens af, at cyberkriminelle inficerer kritiske systemer med eksempelvis ransomware, eller hvis et ransomwareangreb mod administrative netværker vanskeliggør kontrol og vedligeholdelse af kritiske systemer. Destruktive cyberangreb kan forstås som cyberangreb, hvor den forventede effekt fx er skade på personer eller fysiske objekter, eller ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning. Denne type cyberangreb må siges at udgøre en trussel mod forsyningssikkerheden. CFCS vurderer dog, at truslen fra destruktive cyberangreb mod energisektoren er lav.

I EnergiCERTs trusselsvurdering for energisektoren fra oktober 2022 har EnergiCERT set på trusselbilledet og tendenserne hos deres medlemmer. EnergiCERT peger på, at der er en generel risiko for alvorlig hackingaktivitet, malware eller anden ondsindet aktivitet. Endvidere nævnes det, at der er potentiale for skadelige cyberaktiviteter, men EnergiCERT forventer ikke, at det giver anledning til påvirkning af kritisk infrastruktur.
Data indsamlet af Deloitte på vegne af Miljøstyrelsen viser, at 'phishing angreb' og 'ransomware' nævnes som eksempler på, hvad forsyningsselskaberne oplever som de væsentligste it-relaterede sikkerhedstrusler for deres virksomhed.

5. Styrket indsats for cyber- og informationssikkerheden i vandsektoren

Miljøstyrelsen etablerer en decentral cyber- og informationssikkerhedsenhed pr. 1. januar 2023. Foruden enhedens obligatoriske opgaver har Miljøstyrelsen iværksat seks konkrete initiativer for yderligere at understøtte cyber- og informationssikkerheden i vandsektoren. På længere sigt forventes yderligere styrkelse på området, når Danmark skal implementere en ny version af EU's Net- og Informationssikkerhedsdirektiv (NIS2-direktivet).

5.1 Miljøstyrelsens cyber- og informationssikkerhedsenhed

Miljøstyrelsen har i forbindelse med implementeringen af regeringens cyber- og informationssikkerhedsstrategi fået til opgave at etablere en decentral enhed for cyber- og informationssikkerhed for vandsektoren (DCIS). Det er et krav til enheden, at enheden har en operativ kapacitet. Konkret betyder det, at enheden skal kunne rapportere til CFCS' situationscenter om status i forbindelse med hændelser og relevante afhængigheder til andre samfundsvigtige funktioner. Enheden skal kunne modtage og forstå varsler samt videreformidle disse til de relevante aktører med henblik på, at aktørerne iværksætter konkret håndtering af varslet, hvis relevant. Enheden skal samarbejde på tværs af ministerområder i hændelsessituationer og indgå i et nationalt it-beredskab. Enheden skal være bemandet i dagtimerne og deltage i en årlig national cyberberedskabsøvelse. Endelig skal enheden planlægge, tilrettelægge og gennemføre en årlig sektorspecifik cyberberedskabsøvelse på ministerområdet.

Foruden de obligatoriske opgaver har Miljøstyrelsen udvalgt seks selvstændige initiativer, der skal gennemføres som led i nærværende strategi. Initiativerne er valgt på baggrund af en brutliste af initiativer, der er blevet skabt i dialog med blandt andre DANVA og Danske Vandværker. Der har været fokus på initiativer, der er realiserbare inden for strategiens tidshorisont 2023-2025 og som på en omkostningseffektiv måde bidrager til cyber- og informationssikkerheden i vandsektoren. Initiativerne indeholder ikke krav til forsyningsselskaberne, og er derved frivillige, men flere af initiativerne indeholder anbefalinger. Eksempelvis indeholder initiativ 1 "It-sikkerhedspolitik" og initiativ 2 "It-beredskabsplan" ikke krav til forsyningsselskaberne om at udarbejde en it-sikkerhedspolitik eller en it-beredskabsplan, men initiativerne skal facilitere, at forsyningsselskaberne udarbejder disse. Initiativerne henvender sig til alle forsyningsselskaber i vandsektoren, dvs. ikke kun de forsyningsselskaber, der aktuelt er defineret som kritisk it-infrastruktur. Det betyder blandt andet, at Miljøstyrenses decentrale cyber- og informationssikkerhedsenhed anbefaler, at alle forsyningsselskaber udarbejder en it-sikkerhedspolitik og en it-beredskabsplan.

Selvom denne strategi ikke indeholder krav, så vil der kunne komme krav til vandsektoren, blandt andet som følge af den kommende implementering af NIS2-direktivet, se afsnittet "Implementering af EU-lovgivning". Det bemærkes endvidere, at der vil ske en yderligere kortlægning af kritisk it-infrastruktur, se afsnittet "Initiativ 5: Yderligere kortlægning af kritisk it-infrastruktur".

Formålet med initiativerne er at bidrage til opfyldelse af følgende strategiske mål i "National strategi for cyber- og informationssikkerhed 2022-2024": 1. Robust beskyttelse af de samfundsvigtige funktioner, 2. Øget kompetenceniveau og ledelsesforankring og 3. Styrkelse af det offentligt-private samarbejde. Nedenfor er vist et overblik sammenhængen mellem strategiens strategiske mål, initiativer og aktiviteter.

I forbindelse med den årlige revision og revidering af arbejdsprogrammet vil der blive taget stilling til justeringer af eksisterende initiativer og etablering af nye. Dette vil ske i takt med at modenhedsniveauet for kompetence øges. Det kunne eksempelvis være hjælp til øget it-sikkerhedsbevidsthed og krav om adskillelse af it- og OT-systemer i vandsektoren.

Strategisk mål	Initiativer	Aktiviteter
Robust beskyttelse af de samfundsvigtige funktioner	**En decentral cyber- og informationssikkerhedsenhed med operationel kapacitet *(obligatorisk)***	• Rapportere til CFCS' situationscenter om status i forbindelse med hændelser og relevante afhængigheder til andre samfundsvigtige funktioner • Kunne modtage og forstå varsler samt videreformidle disse til de relevante aktører med henblik på, at aktørerne iværksætter konkret håndtering af varslet, hvis relevant • Samarbejde på tværs af ministerområder i hændelsessituationer og indgå i et nationalt it-beredskab • Være bemandet i dagtimerne • Deltage i en årlig national cyberberedskabsøvelse • Planlægge, tilrettelægge og gennemføre en årlig sektorspecifik cyberberedskabsøvelse på ministerområdet
	Yderligere kortlægning af kritisk it-infrastruktur (initiativ 5)	• Definere parametre og metode til identifikation af evt. yderligere kritisk it-infrastruktur. • Gennemgang af vandsektorens selskaber med henblik på kortlægning af yderligere kritisk it-infrastruktur.
	Anbefalinger til vandsektoren om konkrete tiltag (initiativ 6)	• Analysere og afdække hvilke anbefalinger om konkrete tiltag, der bør gives til vand- og spildevandsselskaber angående kritisk it-infrastruktur. • Udmelding om konkrete tiltag, som Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed anbefaler, at alle vand- og spildevandsselskaber med kritisk it-infrastruktur implementerer.
Øget kompetenceniveau og ledelsesforankring	**It-sikkerhedspolitik (initiativ 1)**	• Indsamle eksempler på it-sikkerhedspolitikker og analysere eksisterende it-sikkerhedspolitikker på tværs af vandsektoren. • Udarbejde en standardskabelon for it-sikkerhedspolitik for vand- og spildevandsforsyningsselskaber. • Løbende dialog med brancheorganisationer med henblik på at udbrede anvendelsen af standardskabelonen for it-sikkerhedspolitik
	It-beredskabsplan (initiativ 2)	• Indsamle eksempler på og analysere eksisterende beredskabsplaner vedrørende cyber- og informationssikkerhed på tværs af vandsektoren. • Udarbejde en standardskabelon for en beredskabsplan for cyber- og informationssikkerhed for vand- og spildevandsforsyningsselskaber, og løbende opdatere denne beredskabsplan. • Løbende dialog med brancheorganisationer med henblik på at udbrede anvendelsen af standardskabelonen for en beredskabsplan for cyber- og informationssikkerhed med særligt fokus på de forsyninger, der har en kritisk it-infrastruktur.
Styrkelse af det offentligt-private samarbejde	**Styrket samarbejde mellem Miljøstyrelsen og**	• Etablering af faste møder mellem Miljøstyrelsen, Energistyrelsen og EnergiCERT med henblik på tæt løbende koordinering mellem myndigheder og CERT.

	vandsektoren (initiativ 3)	• Etablering af faste møder mellem Miljøstyrelsen, DANVA og Danske Vandværker med henblik på tæt løbende koordination mellem myndigheder og brancheorganisationer. • Etablering af referencegruppe, der følger og giver inputs til den decentrale cyber- og informationssikkerhedsenheds arbejde. Referencegruppen mødes som minimum to gange årligt.
	Koordinering med EnergiCERT (initiativ 4)	• Løbende koordinering og afklaring af snitflader mellem EnergiCERT og MST-DCIS. • Understøtte udviklingen af EnergiCERT.

5.1.1 Initiativ 1: It-sikkerhedspolitik

Miljøstyrelsen anbefaler, at alle selskaber med it tilkoblet vandforsyningen udarbejder en it-sikkerhedspolitik. Vandselskaber skal forholde sig til trusselsbilledet for at undgå cyberangreb og nedbrud. Cyberangreb er en alvorlig trussel mod forsyningssikkerheden, og Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed anbefaler derfor, at forsyningsselskaberne laver en passende risikovurdering af egne it-systemer og udarbejder en passende it-sikkerhedspolitik. En nedskrevet it-sikkerhedspolitik er et vigtigt element i arbejdet med at styrke cybersikkerheden og forebygge cyberangreb. En it-sikkerhedspolitik sikrer at både ledelsen og medarbejderne har mulighed for at forstå, hvordan virksomheden forholder sig til it-sikkerhed. It-sikkerhedspolitikken har på den måde til formål, at sætte rammerne for forsyningsselskabet på et overordnet niveau. Den indeholder de overordnede målsætninger og placerer det overordnede ansvar for cyber- og informationssikkerheden i forsyningsselskabet. Som udgangspunkt bør it-sikkerhedspolitikken være kortfattet og kan ses som et ledelsesnotat med ambitioner for forsyningsselskabets arbejde med cybersikkerhed. It-sikkerhedspolitikken udgør fundamentet for, at forsyningsselskabet kan udarbejde retningslinjer for it-anvendelsen, som er konkrete og implementerbare.

Miljøstyrelsen vil udarbejde en standardskabelon for it-sikkerhedspolitik, der kan adopteres og implementeres af alle vandselskaber i vandsektoren. Standardskabelonen vil med andre ord skulle tilpasses det enkelte selskabs behov og kritikalitet, og vil give selskaberne et godt udgangspunkt for at udarbejde deres egen it-sikkerhedspolitik. Den centrale forankring skal sikre at it-sikkerhedspolitikken holdes opdateret og relevant i takt med at trusselsbilledet i sektoren ændrer sig, samt i forhold til den stigende digitalisering i vandsektoren.

Som beskrevet ovenfor er det vigtigt med en sikkerhedspolitik. Det er dog udmøntningen af it-sikkerhedspolitikken i konkrete retningslinjer og procedurer, der konkret skal beskrive, hvordan vand- eller spildevandsforsyningen i dagligdagen forebygger, identificerer og håndterer et cyberangreb og efterfølgende genopretter systemerne. Her vil der blive skabt anbefalinger til procedure og retningslinjer.

Det er væsentligt at niveauet for skabelonen tager højde for, at forsyningsselskaberne er meget forskellige. Der vil derfor i forbindelse med udarbejdelsen af skabelonen blive set på, om der bør være flere versioner, eller om der kan gøres andet for at skabelonen hurtigt kan tilpasses til den enkelte forsyning.

Nedenfor er vist konkrete aktiviteter, som Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed vil gennemføre, som elementer i initiativet.

Konkrete aktiviteter
Indsamle eksempler på it-sikkerhedspolitikker og analysere eksisterende it-sikkerhedspolitikker på tværs af vandsektoren.
Udarbejde en standardskabelon for it-sikkerhedspolitik for vand- og spildevandsforsyningsselskaber.
Løbende dialog med brancheorganisationer med henblik på at udbrede anvendelsen af standardskabelonen for it-sikkerhedspolitik

5.1.2 Initiativ 2: It-beredskabsplan

Ligesom med it-sikkerhedspolitikken er det op til det enkelte forsyningsselskab at udarbejde en passende beredskabsplan. Det er Miljøstyrelsens klare anbefaling, at alle forsyningsselskaber har en beredskabsplan og genopretningsplaner, og det er ligeledes vigtigt, at beredskabsplanen forholder sig til brud på cyber- og informationssikkerheden.

Ensartede beredskabsplaner for vandselskaber, der testes løbende, bidrager til at sikre, at vandselskaber kan forblive operationelle i tilfælde af cyberangreb, der rammer it- eller OT-systemer. Dette vil være med til overordnet at styrke forsyningssikkerheden i Danmark, samt minimere risici i vandsektoren forbundet med cyberangreb.

Initiativet skal understøtte, at der udarbejdes klare og brugbare beredskabsplaner for håndtering af cyberangreb, som kan sikre, at vandforsyningsselskaberne kan forblive operationelle.

For at understøtte en udvikling i denne retning vil Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed ligesom for it-sikkerhedspolitikken udarbejde en eller flere standardskabeloner, der kan adopteres og implementeres af alle vandselskaber i vandsektoren. Standardskabelonen vil med andre ord skulle tilpasses det enkelte selskabs behov, og give selskaberne et godt udgangspunkt for at udarbejde deres egen beredskabsplan for it-infrastruktur. Den centrale forankring skal sikre, at skabelonen for en beredskabsplan for it-infrastruktur holdes opdateret og relevant i takt med, at trusselsbilledet i sektoren ændrer sig, samt i forhold til den stigende digitalisering i vandsektoren.

Det er væsentligt at niveauet for skabelonen tager højde for, at forsyningsselskaberne er meget forskellige. Der vil derfor i forbindelse med udarbejdelsen af skabelonen blive set på, om der bør være flere versioner, eller om der kan gøres andet for at skabelonen hurtigt kan tilpasses til den enkelte forsyning.

Nedenfor er vist konkrete aktiviteter, som Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed vil gennemføre som elementer i initiativet.

Konkrete aktiviteter
Indsamle eksempler på og analysere eksisterende beredskabsplaner vedrørende cyber- og informationssikkerhed på tværs af vandsektoren.
Udarbejde en standardskabelon for en beredskabsplan for cyber- og informationssikkerhed for vand- og spildevandsforsyningsselskaber, og løbende opdatere denne beredskabsplan.
Løbende dialog med brancheorganisationer med henblik på at udbrede anvendelsen af standardskabelonen for en beredskabsplan for cyber- og informationssikkerhed med særligt fokus på de forsyninger, der har en kritisk it-infrastruktur.

5.1.3 Initiativ 3: Styrket samarbejde mellem Miljøstyrelsen og vandsektoren

Kompleksiteten i vandsektoren er stor i forhold til både drift, anlæg, it- og OT-systemer mv. Kompleksiteten forstærker behovet for en dybere forståelse og tættere samarbejde mellem Miljøstyrelsen og vandsektoren. I vandsektoren har brancheorganisationerne DANVA og Danske Vandværker bidraget til arbejdet med cyber- og informationssikkerhed for forsyningsselskaber af alle størrelser, gennem tilbud som vidensdeling og sparring, cybernetværk, kurser, og it-sikkerhedstilbud. Brancheorganisationerne har tæt dialog med vandselskaberne på tværs af vandsektoren og besidder central indsigt og viden om deres medlemmer, som kan bidrage til det fremtidige arbejde med cyber- og informationssikkerhed. Initiativet har til formål af fastholde og styrke det eksisterende samarbejde mellem Miljøstyrelsen (DCIS) og brancheorganisationerne (DANVA og Danske Vandværker). Der etableres derfor et forum, hvor Miljøstyrelsen, DANVA og Danske Vandværker mødes fast med henblik på at koordinere, dele viden og håndtere udfordringer med cyber- og informationssikkerhed.

Energistyrelsen har allerede etableret en decentral cyber- og informationssikkerhedsenhed inden for energiforsyning, og enheden kan således være en væsentlig sparringspartner for Miljøstyrelsen i arbejdet med cyber- og informationssikkerhed på forsyningsområdet. EnergiCERT arbejder allerede aktivt med netværksmonitorering, deling af trusler, hændelsesregistrering, kurser etc., og EnergiCERT vil derfor ligeledes være en central sparrings- og samarbejdspartner for Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed. Endvidere bliver DANVA medlem af EnergiCERT fra 2023. For at håndtere de løbende problemstillinger bedst muligt på området for cyber- og informationssikkerhed etableres der med dette initiativ et forum, hvor Miljøstyrelsen, Energistyrelsen og EnergiCERT mødes fast.

Derudover etableres der en referencegruppe, der følger og giver input til arbejdet i Miljøstyrelsens cyber- og informationssikkerhedsenhed. Referencegruppen mødes som minimum to gange årligt.

Nedenfor er vist konkrete aktiviteter, som Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed vil gennemføre, som elementer i initiativet.

Konkrete aktiviteter
Etablering af faste møder mellem Miljøstyrelsen, Energistyrelsen og EnergiCERT med henblik på tæt løbende koordinering mellem myndigheder og CERT. Etablering af faste møder mellem Miljøstyrelsen, DANVA og Danske Vandværker med henblik på tæt løbende koordination mellem myndigheder og brancheorganisationer.
Etablering af referencegruppe, der følger og giver inputs til den decentrale cyber- og informationssikkerhedsenheds arbejde. Referencegruppen mødes som minimum to gange årligt.

5.1.4 Initiativ 4: Koordinering med EnergiCERT

Vandsektorens kompleksitet og den stigende trussel mod cyber- og informationssikkerheden har øget behovet for nye krav til myndighederne. Samtidig er der behov for øget samarbejde på tværs af sektoren om bl.a.

- vidensdeling,
- monitorering af hændelser,
- løbende vurdering af cybertruslen,
- og ikke mindst at stille beredskab og ressourcer tilgængeligt når hændelser er indtruffet.

Ligeledes stilles der krav til myndighederne om at sikre det rette fundament af uddannelse samt om rådgive og vejlede vandselskaberne i arbejdet med sektorspecifik cyber- og informationssikkerhed.

I energisektoren har man etableret en fælles sektorCERT, kaldet EnergiCERT. CERT står for Computer Security Incident Response Team. EnergiCERT er en non-profit forening, der i dag hjælper over 400 energiselskaber med cybersikkerhed. Denne finansieres ved, at de stiftende organisationers medlemmer betaler til EnergiCERT via deres medlemsbidrag til organisationerne, og derudover betaler det enkelte energiselskab for udvalgte ydelser på frivillig basis. EnergiCERT tilbyder en lang række ydelser til sine medlemmer, herunder netværksmonitorering, kurser i OT-sikkerhed, hændelseshåndtering ved cyberangreb etc. EnergiCERT har etableret et digitalt SektorForum, hvor medlemmer kan få hjælp og vejledning fra både EnergiCERT og andre medlemmer.

EnergiCERT kan bistå vandsektoren og Miljøstyrelsen som sektormyndighed med at løfte niveauet for cyber- og informationssikkerhed i vandsektoren. Dette er bl.a. årsagen til at DANVA har valgt at blive en del af EnergiCERT fra år 2023. Det er muligt at indgå individuelle i medlemskaber hos EnergiCERT, hvilket åbner for, at forsyningsselskaber kan blive medlem hos EnergiCERT, uanset om de er medlem hos DANVA eller ej.

Dette initiativ indebærer, at der skal være en tæt dialog mellem Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed og EnergiCERT. Dels i forhold til at afklare de indbyrdes snitflader, dels i forhold til at understøtte udviklingen af EnergiCERT.

Nedenfor er vist konkrete aktiviteter, som Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed vil gennemføre, som elementer i initiativet.

Konkrete aktiviteter
Løbende koordinering og afklaring af snitflader mellem EnergiCERT og MST-DCIS.
Understøtte udviklingen af EnergiCERT

5.1.5 Initiativ 5: Yderligere kortlægning af kritisk it-infrastruktur

Aktuelt har Miljøstyrelsen defineret den kritiske it-infrastruktur som OT-systemerne hos multiforsyningsselskaber og alle store selskaber samt alle kommunale spildevandsselskaber. Ved multiforsyningsselskaber forstås selskaber med over 800.000 m^3 vandmængder årligt og yderligere forsyningsarter, og ved store selskaber forstås selskaber med over 800.000 m^3 producerede vandmængder årligt. Der er en risiko for, at der med disse afskæringskriterier er selskaber, hvis it-infrastruktur i dag ikke er defineret som kritisk, men som burde være det. Miljøstyrelsen vil gennemføre en mere detaljeret kortlægning, for at afdække, om den nuværende liste over kritisk it-infrastruktur bør udvides.

Der skal gennemføres en yderligere kortlægning af kritisk it-infrastruktur i vandsektoren. Kortlægningen bør skelne til Forsvarsministeriets retningslinjer for, hvornår infrastruktur er kritisk infrastruktur som beskrevet under afsnit *2.3 Kritisk infrastruktur og it-infrastruktur* i vandsektoren. Kortlægningen bør foretages ud fra så objektive parametre som muligt, når den kritiske infrastruktur kortlægges, og der bør i kortlægningen tages hensyn til branchespecifikke parametre. Blandt de branchespecifikke parametre, der kan være værd at medtage i kortlægningen kan nævnes ”Andel af samlet vandmængde i sektoren”, ”Antal forbrugere”, ”Substitutionsmuligheder”, ”Geografisk spredning” og ”Betydning for øvrige samfundsvigtige funktioner”. Det er endvidere afgørende, at der tages højde for NIS2-direktivet i forbindelse med kortlægningen,

således at der ikke er nogen uoverensstemmelser mellem, hvad kortlægningen kommer frem til, og hvad der fremgår af NIS2-direktivet for så vidt angår omfattede forsyninger.
Nedenfor er vist konkrete aktiviteter, som Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed vil gennemføre, som elementer i initiativet.

Konkrete aktiviteter
Definere parametre og metode til identifikation af evt. yderligere kritisk it-infrastruktur.
Gennemgang af vandsektorens selskaber med henblik på kortlægning af yderligere kritisk it-infrastruktur.

5.1.6 Initiativ 6: Anbefalinger til vandsektoren om konkrete tiltag

Vand- og spildevandsforsyninger har brug for konkrete og operationelle anbefalinger i forhold til, hvordan cyber- og informationssikkerheden styrkes og vedligeholdes. Samtidig har det analysearbejde, som Miljøstyrelsen har foretaget i samarbejde med Deloitte, peget på, at en af de største barrierer for at styrke cybersikkerheden i vandsektoren, er sammenkoblingen af it- og OT-systemer.

Der findes allerede mange gode anbefalinger til, hvordan cyber- og informationssikkerheden styrkes. Eksempelvis har alle statslige myndigheder siden 2020 skulle efterleve 20 tekniske minimumskrav for at sikre et højt cyber- og informationssikkerhedsniveau. I "Håndbog om EnergiCERTs trusselsvurderinger" er der udarbejdet 25 konkrete anbefalinger til aktører inden for kritisk infrastruktur, som EnergiCERT anbefaler bliver implementeret uanset det aktuelle trusselsniveau. Center for Cybersikkerhed kommer også med anbefalinger til, hvordan cyber- og informationssikkerheden kan styrkes. Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed vil arbejde på at koordinere enhedens anbefalinger med de eksisterende aktører som fx EnergiCERT og Center for Cybersikkerhed.

Med udgangspunkt i disse og andre eksisterende anbefalinger, vil Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed vurdere, hvilke anbefalinger der bør gælde for vandsektoren. Det er muligt, at det viser sig, at EnergiCERTs aktuelle 25 anbefalinger til energisektoren er samme anbefalinger, som der bør gives til vandsektoren, men dette skal i første omgang afklares nærmere.

Nedenfor er vist konkrete aktiviteter, som Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed vil gennemføre som elementer i initiativet.

Konkrete aktiviteter
Analysere og afdække hvilke anbefalinger om konkrete tiltag, der bør gives til vand- og spildevandsselskaber angående kritisk it-infrastruktur.
Udmelding med anbefalinger til vandsektoren om konkrete tiltag, som Miljøstyrelsens decentrale cyber- og informationssikkerhedsenhed anbefaler, at alle vand- og spildevandsselskaber med kritisk it-infrastruktur implementerer.

5.2 Implementering af EU-lovgivning

Direktivet om net- og informationssikkerhed (NIS-direktivet) regulerer virksomheder og myndigheder på cyber- og informationssikkerhedsområdet. Direktivet bliver udmøntet i nationale bekendtgørelser og fungerer som bindende lov, hvilket betyder, at selskaber skal efterleve kravene i bekendtgørelsen.

Med vedtagelse af det nye net- og informationssikkerhedsdirektiv (NIS2-direktivet) udvides omfanget af virksomheder og organisationer, der bliver omfattet af direktivet. Drikkevand- og spildevandsområdet er omfattet af NIS2-direktivet, og det er forventningen, at implementeringen af NIS2-direktivet kan få væsentlig betydning for en del af vandforsynings- og spildevandsselskaberne.

NIS2-direktivet har til formål at sikre en mere ensartet tilgang til cyber- og informationssikkerhed på tværs af medlemslandene. Direktivet fokuserer bl.a. på, at der skal anlægges en risikobaseret tilgang til cyber- og informationssikkerhed, og der stilles krav om, at direktioner i kritiske vandforsynings- og spildevandsselskaber jævnligt modtager relevant uddannelse i cybersikkerhed og desuden står til ansvar for beslutninger vedrørende cyber- og informationssikkerhed. Hertil kommer en række krav til virksomhedernes forebyggelse og håndtering er cybersikkerheds-hændelser, samt rapportering om hændelser til myndighederne.

NIS2-direktivet er ikke adresseret endeligt i form af konkrete initiativer i denne strategi, da der fortsat ikke er fuld klarhed over, hvordan direktivet skal implementeres i dansk lovgivning. Det vil dog i forbindelse med den årlige revision og revidering af strategien være muligt at tilpasse arbejdsprogrammet i relation til implementeringen af direktivet. Det forventes, at direktivets krav skal være implementeret ultimo 2024.

6. Arbejdsprogram

Miljøstyrelsen har som den ansvarlige sektormyndighed ansvaret for, at styrke cyber- og informationssikkerheden i vandsektoren via både de obligatoriske opgaver og identificerede tiltag.

6.1 Tidshorisont

For at følge, evaluere og styre processen for implementeringen af de beskrevne initiativer, vil referencegruppen følge den decentrale cyber- og informationssikkerhedsenheds arbejde og tidsplanen for arbejdet.

I arbejdsprogrammet vil referencegruppen som det første blive inddraget i en mere detaljeret plan for implementering af initiativerne på kort og mellemlang sigt. Endvidere vil referencegruppen på sigt inddrage flere relevante tiltag for løbende at løfte modenheden for Miljøstyrelsens DCIS for vandsektoren.

Med forbehold for ændringer beskrives nedenfor, hvad der må forventes gennemført, på kort sigt (2023) og mellemlang sigt (2024-2025)

Initiativer	2023 1. halvår	2. halvår	2024 1. halvår	2. halvår	2025 1. halvår	2. halvår
1. It-sikkerhedspolitik						
2. Beredskabsplaner						
3. Styrket samarbejde mellem MST og vandsektoren						
4. EnergiCERT						
5. Yderligere kortlægning af kritisk it-infrastruktur						
6. Anbefalinger til vandsektoren om konkrete tiltag						

7. Årlig revision og revidering

7.1 Årlig revision og revidering

Der er sket meget i året 2022, hvor Ukraine-krigen, energikrisen i Europa og gaslækagerne i Østersøen har skabt et fornyet og ekstraordinært fokus på, hvordan vi understøtter forsyningssikkerheden bredt set.

Det er samtidig den hastige udvikling på cybersikkerhedsområdet, der gør det nødvendigt hele tiden at tilpasse sig den løbende udvikling. I takt med at cybersikkerheden styrkes, bliver de kriminelle også dygtigere. De finder nye sårbarheder, og de angreb, der kan udføres, tager nye former.

Heller ikke på reguleringssiden står tingene stille. Med den nye version af EU's Net- og Informationssikkerhedsdirektiv (NIS2-direktivet), står vi også over for væsentlige forandringer reguleringsmæssigt, når direktivet skal implementeres i dansk lovgivning. Det er ikke på nuværende tidspunkt muligt at sige, hvordan direktivet konkret vil blive udmøntet i forhold til bl.a. krav og tilsyn.

Det er bl.a. på baggrund af ovenstående, at det er nødvendigt løbende at tilpasse arbejdsprogrammet og tidsplanen. For at sikre strategiens fortsatte relevans vil referencegruppen én gang årligt revidere det strategiske arbejde, se fremad og forholde sig til nye tiltag og den cybersikkerhedsmæssige udvikling i vandsektoren. På baggrund heraf vil strategien blive tilpasset, udviklet eller videreført uændret.

Strategi for cyber- og informations-sikkerhed i vandsektoren 2023-2025

Miljøstyrelsen
Tolderlundsvej 5
5000 Odense C

www.mst.dk