Miljø- og
Ligestillingsministeriet
Miljøstyrelsen

Vejledning til vandsektoren om foranstaltninger

Vejledning, nr. 87

April 2026

Udgiver: Miljøstyrelsen

Redaktion: Miljøstyrelsen

ISBN: 978-87-7564-101-7

Indhold

Indledning

NIS 2-lovens § 6 om ”Foranstaltninger til styring af cybersikkerhedsrisici” stiller omfattede krav til vand- og spildevandsforsyninger. Kravene berør enheders tekniske, operationelle og organisatoriske foranstaltninger til styring af risici for sikkerheden i net- og informationssystemer, der anvendes til levering af vand- og spildevandsforsyningernes tjenester. Miljøstyrelsens har udarbejdet ”Vejledning til vandsektoren om foranstaltninger” med det formål, at vejlede NIS 2-omfattede vand- og spildevandsforsyninger i overholdelsen af kravene i loven, ved angivelse af sektorspecifikke anbefalinger til enheders foranstaltninger.

Miljøstyrelsens vejledning skal ses som et supplement til Styrelsen for Samfundssikkerheds (SAMSIK) vejledning til implementering af cybersikkerhedsforanstaltninger. Derfor vil Miljøstyrelsens vejledning skulle læses indenfor rammerne af SAMSIKs vejledning. Miljøstyrelsens vejledning beskriver, hvad vand- og spildevandsforsyningerne bør og med fordel kan implementere med udgangspunkt i vandsektorens særlige net- og informationssystemskendetegn. Da Miljøstyrelsens vejledning er et supplement, antages det, at læseren er orienteret i SAMSIKs vejledning, og har kendskab til NIS 2-lovens krav om foranstaltninger.

Miljøstyrelsens ”Vejledning til vandsektoren om foranstaltninger” er skrevet med henblik på de vand- og spildevandsforsyninger, som er omfattet af NIS 2-loven, i forlængelse af Miljøstyrelsens vejledning til vandsektoren om anvendelsesområdet.

1. Hvad kendetegner net- og informationssystemer i vandsektoren?

Vandsektoren har visse kendetegn, som er relevante for implementeringen af NIS 2-lovens krav om foranstaltninger. Vandsektoren i Danmark er bl.a. kendetegnet ved

- En decentraliseret struktur med vand- og spildevandsvirksomheder af varierende størrelser, som drifter autonomt.
- Automatisering, typisk via OT-systemer m.v., som opretholder den daglige drift på vand- og spildevandsvirksomheder.

Jævnfør SAMSIKs *vejledning til implementeringen af NIS 2-lovens cybersikkerhedsforanstaltninger* skal NIS 2-lovens foranstaltninger implementeres for at opnå **passende** niveau af sikkerhed i forhold til leveringen af de ydelser, som gør, at enheder er omfatter af NIS 2-loven. Det er Miljøstyrelsens vurdering, at NIS 2-lovens krav om foranstaltninger i vandsektoren bør inkludere beskyttelse af vand- og spildevandsenheders OT-systemer, grundet OT-systemers vigtighed i leveringen af ydelser. Miljøstyrelsens vedledning og anbefalinger heri, er derfor centreret omkring beskyttelse af OT-systemer og dets tilhørende IT. Som konsekvens heraf, vil Miljøstyrelsens vejledning ikke udelukkende fokusere på traditionel cybersikkerhed, og vil berøre de fysiske aspekter af enheders sikkerhed.

2. Sikkerhedsstandarder

SAMSIK har i deres vejledning vedlagt referencer til fem forskellige internationale sikkerhedsstandarder og rammeværk. Miljøstyrelsen fremhæver tre udvalgte sikkerhedsstandarder, som værende særligt værdiskabende for forsyningsenheder omfattet af NIS 2-lovens krav om foranstaltninger. De tre udvalgte sikkerhedsstandarder er

- ISO/IEC 27001:2023
- CIS Critical Security Controls
- IEC 62443

De to udvalgte standarder ISO/IEC 27001:2023 og IEC 62443 er inkluderet i SAMSIKs "vejledning til implementering af foranstaltninger", mens CIS Critical Security Controls er udeladt. Miljøstyrelsen har derfor i Bilag A inkluderet en liste over relevante afsnit i CIS Critical Security Controls lig de lister, som SAMSIK har inkluderet i deres vejledning.

2.1 Hvorfor anvende en sikkerhedsstandard?

Miljøstyrelsen anbefaler, at vand- og spildevandsforsyningsenheder omfattet af NIS 2-lovens krav om foranstaltninger anvender sikkerhedsstandarder som rammesættende redskaber i forbindelse med implementeringen af NIS 2-lovens krav. Sikkerhedsstandarder er praktiske på baggrund af følgende årsager:

- **En struktureret fremgangsmåde:** En rammesættende sikkerhedsstandard kan assistere ifm. enhedens risikobaseret tilgang, ved at belyse relevante ræsonnementer og konkretisere, hvilke tiltag enheden kan implementere, samt hvilke effekter tiltagene bør have. Derved, kan en sikkerhedsstandard være behjælpelig med at sikre, at enhedens indsatser skaber de sikkerhedsmæssige forbedringer, som NIS 2-loven kræver.
- **Fælles forståelser:** Sikkerhedsstandarder giver anledning til skabelsen af fælles sikkerhedsforståelser internt i enheden, mellem enheder og med eksterne interessenter. Samarbejder mellem disse styrkes derved via forenkling og tydeliggørelse af bl.a. roller, procedurer og mål. Miljøstyrelsen vurderer, at en sådan fremgangsmåde udnytter de cybersikkerhedsmæssige fordele, som følger af vandsektorens decentraliserede struktur, ved at fremme vidensdeling på tværs af vandsektoren, mens cybersikkerhedstiltag eksekveres på enhedsniveau.
- **Eksterne certifikater og akkrediteringer:** Hvis vand- og spildevandsforsyninger ønsker at anvende ekstern rådgivning eller akkreditering i forbindelse med implementering og overholdelse af NIS 2-lovens krav, kan anvendelsen af anerkendte sikkerhedsstandarder muliggøre eksterne evalueringer. Det er væsentligt, at enheden sikrer kongruens mellem NIS 2-lovens krav og vurderingsgrundlaget af enhedens sikkerhedsstandardimplementering, fx via et *Statement of Applicability* (SoA), hvis ekstern akkreditering af en sikkerhedsstandard ønskes anvendt som basis for lovoverholdelse. Dette er centralt, da anvendelse af en sikkerhedsstandard i sig selv ikke er en garanti for opfyldelse af NIS 2-lovens krav.

2.2 Hvordan anvendes sikkerhedsstandarder?

Miljøstyrelsen anbefaler, at enheden starter processen med først at danne overblik over enhedsaktiver, som vil kunne påvirke net- og informationssystemer. Dette anbefales da passende implementeringer af NIS 2-lovens krav afhænger af enhedens behov og af enhedens udgangspunkt. Det er væsentligt, at enheden inkluderer alle relevante aktiver, heraf også relevante produktionssystemaktiver, grundet tendenser til digitalisering af disse.

Redskaber, såsom systemoverblikket på Sikkerdigital.dk, kan være behjælpelige. Vær dog opmærksom på, at dette redskab er generisk og derfor ikke nødvendigvis skaber et fyldestgørende overblik, når det gælder en vand- eller spildevandsforsyningsenhed.

Alle sikkerhedsstandarder som Miljøstyrelsen anbefaler, præsenterer egne trinvise fremgangsmåder. Miljøstyrelsen anbefaling til enhedens anvendelse af standarderne er, at enheden følger disse fremgangsmåder som udgangspunkt, men undlader en kronologisk rækkefølge, hvis det vurderes fordelagtigt.

Miljøstyrelsen anbefaler derudover, at enheden orienterer sig om hver sikkerhedsstandard, da standarderne deler flere kendetegn på tværs, men kan være forskellige henset til bl.a. formål, kompleksitet og omfang. Det er fordelagtigt at have NIS 2-lovens krav in mente og løbende prioritere overholdelsen af dem som et minimum.

2.3 Sikkerhedsstandarder som Miljøstyrelsen anbefaler

Miljøstyrelsen udfolder de tre udvalgte sikkerhedsstandarder, således, at enheden kan få overblik over, hvad der kendetegner hver standard, og til hvilket formål den enkelte anbefales anvendt. Vær opmærksom på, at flere sikkerhedsstandarder, eller i nogle tilfælde enkelte dele af standarder, kan anvendes på samme tid. Selvom standarderne overlapper til en vis grad, kan enheden anvende enkelte sikkerhedsstandarders styrker og svagheder.

Sikkerhedsstandarderne bør derfor ikke nødvendigvis anskues som alternativer, men som enkeltstående redskaber, der hver bedst anvendes med hver deres formål.

2.3.1 ISO/IEC 27001:2023

ISO/IEC 27001:2023 (ISO 27001) er en sikkerhedsstandard til etablering af et ledelsessystem for informationssikkerhed, som stiller systematiske krav til forsyningsenhedens politikker og processer. Implementeringen af ISO 27001 vil berøre adskillige facetter af enheden organisatoriske og digitale infrastruktur, og kan synes omfattende. Miljøstyrelsen fremhæver, at ISO 27001 er en yderst anerkendt sikkerhedsstandard, og er derfor egnet til vidensdeling og akkreditering.

ISO 27001 beskriver hvad enheden bør opnå med sikkerhedsindsatser, men ikke hvordan dette praktisk udføres. Til dette formål findes der adskillige tilføjelser, heriblandt

- ISO/IEC 27002, som yderligere konkretiserer og beskriver, hvordan ISO 27001's sikkerhedstiltag kan implementeres.
- ISO/IEC 27005, som indeholder vejledende risikostyringsredskaber.

Miljøstyrelsen anbefaler anvendelsen af sikkerhedsstandarden ISO 27001, såfremt enheder ønsker at etablere et omfattende cybersikkerhedsrammeværk for hele vand- eller spildevandsforsyningsenheden, eller hvis enheden ønsker ekstern akkreditering.

ISO 27001 er opbygget over samme struktur som øvrige ISO-standarder, heriblandt ISO 9001, og kan derfor forekomme velkendt, såfremt enheden erfaring med standardserien.

ISO 27001 kan købes gennem Dansk Standard.

2.3.2 IEC 62443

IEC 62443 er en sikkerhedsstandardpakke udviklet til industrielle produktionssystem, med henblik på sikkerhed og modstandsdygtighed, således at drift kan opretholdes.

Pakken er konstrueret med henblik på inddeling af sikkerhed i fire inkrementelle sikkerhedsniveauer, varierende fra *Security Level-1* til *Security Level-4*, som indikerer sikkerhedstiltags kompleksitet. Med afsæt i egen risikovurdering kan enheder vurdere, hvilke IEC 62443-sikkerhedsniveauer, der er passende.

Sikkerhedsstandardpakken berører adskillelige aspekter af organisationens produktionssystemssikkerhed, men er tematisk opdelt på baggrund af specifikke formål. Som konsekvens heraf, anbefaler Miljøstyrelsen særligt del 62443-3-3 og del 62443-4-2, da disse vedrører hhv. system- og komponentkrav, med henblik på net- og informationssystemssikkerhed.

Miljøstyrelsen vurderer, at sikkerhedsstandardpakken IEC 62443 er yderst velegnet til vand- og spildevandforsyningsenheder omfattet af NIS 2-loven, på baggrund af standardpakkens fokus på kontinuerlig drift. Da sikkerhedsstandardpakken er skrevet til beskyttelsen af industriel produktion, er det yderligere Miljøstyrelsen vurdering, at IEC 62443 ikke alene kan afdække hele enheders net- og informationssystem. Derfor, kan IEC 62443, særligt del 62443-3-3 og del 62443-4-2, med fordel anvendes I samspil med en generisk sikkerhedsstandard, såsom CIS Critical Security Controls.

IEC 62443 sikkerhedsstandardpakken kan købes på Dansk Standard. Vær opmærksom på, at enkelte dele kan købes enkeltvist, såfremt det ønskes.

2.3.3 CIS Critical Security Controls

CIS Critical Security Controls (CIS Controls) er en sikkerhedsstandard bygget op om 18 kontrolpunkter, som hvert belyser et relevant cybersikkerhedstiltag. Alle 18 kontrolpunkter har fælles opbygning:

- Beskrivelse af det enkelte kontrolpunkt, dets væsentlighed, og hvorfor det forbedrer cybersikkerhed.
- Et overblik over processer og redskaber, som er relevante i forbindelse med kontrolpunktet.
- Detaljerede beskrivelser af de specifikke handlinger, som kan foretages for opfyldelse af kontrolpunktet. CIS Controls kalder disse handlinger *safeguards,* og niveauopdeler dem på baggrund af kompleksitet i tre niveauer.

CIS Controls 18 kontrolpunkter er de mest kritiske kontrolpunkter i net- og informationssystemsikkerhed, og generisk formuleret. Derfor er CIS Controls den mindst omfattende sikkerhedsstandard, som Miljøstyrelsen fremhæver.

På baggrund de 18 kontrolpunkters generiske natur, vurderer Miljøstyrelsen, at CIS Controls er en yderst brugervenlig og konkret sikkerhedsstandard, og anbefaler den som indledende redskab med henblik på vand- og spildevandsforsyningers net- og informationssystemer.

Dog, kan CIS Controls grundet dens generiskhed, forekomme snæver med henblik på total beskyttelse af enheders net- og informationssystemer. Dette skyldes, at standarden er konstrueret med henblik på cybersikkerhed i traditionel netværksstruktur, der ikke nødvendigvis inkluderer OT-systemer eller de karakteristika, som kendetegner vandsektoren.

Derfor anbefaler Miljøstyrelsen, at vand- og spildevandsforsyninger anvender sikkerhedsstandarden IEC 62443 som supplement, heraf særligt del 62433-3-3 og del 62443-4-2, som er konstrueret til formålet produktionssystembeskyttelse i konteksten af net- og informationssystemer. I en sådan konstellation, kan CIS Controls agere som enhedens overordnede net- og informationssystemsrammeværk og metode, med IEC 62443 som supplement specifikt til enhedens OT-system.

CIS Controls gratis at anvende, og kan hentes på Center for Internet Security

3. NIS 2-lovens foranstaltninger

Herunder har Miljøstyrelsen inkluderet vandsektorspecifikke anbefalinger til de enkelte foranstaltningskrav.

3.1 Politik for risikostyring og informationssikkerhed

Det er nødvendigt, at enheder foretager egne risikoanalyser for at bestemme, hvilke foranstaltninger der er passende i den enkelte vand- eller spildevandsforsyning. Miljøstyrelsen anbefaler, at enheden anvender forsyningskritiske aktivers nødvendighed for opretholdelse af drift, som udgangspunktet for formulering af informationssikkerheds- og risikostyringspolitikker. Med fordel kan trusselsvurdering Cybertruslen mod vandsektoren, skrevet af Center For Cybersikkerhed, anvendes i forbindelse med politikkerne.

Ved formuleringen af risikostyrings- og informationssikkerhedspolitikker, kan følgende spørgsmål stilles: *Hvilke konsekvenser er uacceptable for driften, i vores vand- eller spildevandsforsyning?* Konsekvenser som enheden beslutter er uacceptable, er dem enheden bør prioritere, at forhindre ved implementering af foranstaltninger. I tilfælde af, at en hændelse medfører forhindring af enhedens forsyningsforpligtelse, vurderer Miljøstyrelsen, at dette sandsynligvis vil være en uacceptabel konsekvens.

Enhedens politikker for risikostyring og informationssikkerhed bør omfatte hele vand- eller spildevandsforsyningens struktur. Miljøstyrelsen anbefaler derfor, at forsyningens politikker for risikostyring og informationssikkerhed bør indeholde, men ikke nødvendigvis begrænses til enhedens:

- Traditionel digital infrastruktur, både mobilt og stationært
- OT-systemkomponenter med betydning for enhedens net- og informationssystemer, fx PLC'er
- Nuværende sikkerhedsforanstaltninger, så disse kan vurderes i forbindelse med enhedens risikovurdering.
- Serviceleverancer med betydning for enhedens net- og informationssystemer, heraf både digitale leverancer, såsom cloud-services, og produktionsleverancer, såsom SRO-systemer.

Miljøstyrelsen fremhæver, at enheden kan anvende fortegnelser over hardware- og softwareaktiver samt visuelle hjælpemidler, såsom flowdiagrammer, netværksdiagrammer og systemarkitekturdiagrammer, til skabelsen af overblik og fælles forståelse på tværs af enheden.

Når overblik haves, anbefaler Miljøstyrelsen, at enheden overvejer enhedens *single points of failure (SPOF)*. SPOF udgør kritiske knudepunkter eller komponenter i enhedens infrastruktur, hvor kompromitteret sikkerhed vil forårsage totale stop af nødvendige aktiviteter, såsom drift eller nødkommunikation. Anvendes konceptet, SPOF, bør enheden inkludere alle relevante afhængigheder i henhold til enhedens net- og informationssystem, inklusivt fysiske afhængigheder, såsom elforsyning og kritiske tjenesteudbyderleverancer i enhedens forsyningskædesikkerhed.

Miljøstyrelsen fremhæver SPOF, fordi vand- og spildevandsforsyninger kan have unikke muligheder for substituering og redundans i forbindelse med opretholdelsen af forsyningens tjeneste ved hændelser:

- Substituering er muligheden for at erhverve alternative metoder til eksekvering af nødvendige processer, eksempelvis ved at have flere forskellige metoder til nødkommunikation.

- Redundans er muligheden for, at aktiver eller deres afhængigheder kan erstattes af tilsvarende, eksempelvis ved at have et nødlager af kritiske produktionssystemiske komponenter.

Miljøstyrelsen har herunder inkluderet spørgsmål til systemovervejelser ved formulering af enhedens risikovurdering. Vær opmærksom på, der kan være flere relevante spørgsmål end nedenstående, men hvis enheden besvarer nedenstående spørgsmål, så har enheden et stærkt udgangspunkt for risikovurderingen.

- Hvilke data håndterer enhedens systemet?
- Hvilke konsekvenser vil det have, hvis informationen bliver tilgængelig for uvedkommende?
- Hvilken fysiske og produktionsrelevante processer understøttes af systemet?
- Hvilke konsekvenser vil det have, hvis uvedkommende får mulighed for at ændre i systemet eller data?
- Hvilke fysiske og produktionsrelevante processer vil påvirkes af ændringer eller af afbrud?
- I hvilken grad / hvor længe vil enheden kunne undvære systemet?
- Hvem står for driften af de forskellige systemer?
- Hvem kan kontaktes, hvis systemet ikke virker?
- Hvordan foretages der backup af enhedens systemer?
- Hvem har adgang til de forskellige systemer?
- Hvordan påvirkes miljøet af afbrud?

3.2 Håndtering af hændelser

Enheden bør skabe overblik over enhedens digitale infrastruktur, inklusiv OT-systemer og komponenter, samt overblik over ind- og udgående netværksforbindelser, når enheden skal vurdere det nødvendige omfang af logning.

Enheden bør være opmærksom på, at logs har mindsket effektivitet uden monitorering. Ønsker enheden ikke at anvende automatisk monitorering, bør procedurer fastlægges for, hvor ofte logs gennemgås, så brud på sikkerheden opdages.

Udsættes enheden for et forsøgt ondsindet angreb, som mislykkes på grund af en eksisterende sikkerhedsforanstaltning, bør enheder ikke anse denne foranstaltning som værende absolut sikker. Angreb kan forsøges flere gange, hvorfor resultatet af enhedens logning bør kontinuerligt analyseres. Vand- eller spildevandsforsyningsenheden bør være opmærksom på overlevelsesbias ved logning. Dette bør forstås som, at de angreb, der kan spores via logning, ikke nødvendigvis udgør alle angreb, som udsættes for. Der kan forekomme angreb – både succesfulde og ikke-succesfulde – som endnu ikke er opdaget. Derfor anbefaler Miljøstyrelsen, at enheden varetager logs og har automatisk monitorering, men samtidig forholder sig kritisk til de dele af enhedens digitale infrastruktur, som monitoreres.

3.3 Driftskontinuitet

Ved etablering af kontinuitetsplaner anbefaler Miljøstyrelsen, at enheder tager afsæt i risikovurderinger, og prioriterer opretholdelsen af vand- eller spildevandforsyning og de systemer, som er centrale i forbindelse med.

Ved cyberhændelser, bør enheden anvende egen it-beredskabsplan. Digitaliseringsstyrelsens vejledning til it-beredskab er hjælpsom ved formulering og eksekvering af it-beredskabsplaner. Miljøstyrelsen anbefaler, at enheden øver it-beredskabsplaner jævnligt, eksempelvis én gang om året. Især bør procedureøvelser og dilemmaøvelser øves, og efterfølgende evalueret.

Det er centralt, at enhedens beredskabsplan(er) reflekterer hele enhedens digitaliserede infrastruktur, inklusivt produktionssystemer og afbrud på fysiske aktiver, for at opnå effektiv krisestyring ved hændelser. Dette anbefales da hændelser i vandsektoren ikke nødvendigvis kan isoleres til udelukkende digitale eller fysiske hændelser. Skriver enheden beredskabsplaner til separate digitale og fysiske hændelser, er det væsentligt, at overveje samspillet mellem dem.

Vælger enheden eksempelvis, at afhænge af manuel drift som følge af enhedens risikovurdering og it-beredskabsplan, bør dette reflekteres i enhedens fysiske beredskabsplan således overgangen kan supporteres af nødvendige fysiske aktiver. Derfor anbefaler Miljøstyrelsen, at enheden øver beredskabsplaner for både vand- og spildevandshændelser samt andre beredskabsplaner omhandlende fysiske hændelser sammen med enhedens it-beredskabsplaner, for at sikre gensidig støtte og opdage uhensigtsmæssige sammenfald.

3.4 Forsyningskædesikkerhed

Miljøstyrelsen anbefaler, at forsyningen vurderer kongruensen mellem den enkelte leverandørs cybersikkerhedspraksis og enhedens sikkerhedsbehov, med afsæt i enhedens risikovurdering af de tjenester og services, som enheden anvender gennem kunde-leverandøraftaler. Miljøstyrelses anbefaler derfor, at enheden prioriterer forhøjet cybersikkerhed hos leverandører, som leverer tjenester, der er afgørende for enhedens krisestyring, udgør *kritiske SPOF eller har adgang til virksomhedens kritiske aktiver, såsom VPN-udbyderes adgang til digital infrastruktur*.

Prioriteringen af tjenesteudbydere og leverandører vil ikke nødvendigvis være ens for alle vand- og spildevandsforsyningers tjenester, og bør derfor vurderes i den enkelte forsyning.

Miljøstyrelsen er opmærksom på, at visse leverandører anvender tredjeparts revisorerklæringer som dokumentation for, at leverandøren internt overholder og varetager nødvendig cybersikkerhedspraksis. Dette kan være et hjælpsomt redskab for enheden, i forbindelse med sikring af enhedens forsyningskædesikkerhed.

Spørgeskemaer og vejledning fra Sikkerdigital.dk, stil sikkerhedskrav til IT-leverandøren, kan være behjælpelige, hvis enheden søger en struktureret metode til forsyningskædesikkerhed.

3.5 Erhvervelse, udvikling og vedligeholdelse

Enheden bør være orienteret om firmware i enhedens net- og informationssystemer. Det er ikke nødvendigvis alle enhedens produkter, som har behov for løbende firmwareopdateringer, men enheden bør have procedurer for de relevante, da det er risikabelt at anvende produkter med forældet firmware, idet disse kan være mere sårbare over for cybersikkerhedsangreb og fejl. Det er vigtigt at være opmærksom på, at udvalgte produkter kan kræve opdateringer fra tjenesteudbyderen, som enheden ikke kan foretage selvstændigt. Se evt. Foranstaltning 4. forsyningskædesikkerhed, for at sikre, at dette udføres ansvarligt.

Relevante overvejelser:

- Hvilke af enhedens aktiver kan opdateres med firmware?
- Hvor ofte bør enhedens produkter opdateres, og i hvilket omfang kan dette påvirke valget af nye produkter?
- Hvem har ansvaret for at opdatere firmware – enhedens medarbejdere eller tredjepart, fx tjenesteudbyder eller producent?
- Ved enheden hvornår firmware opdateres, således at der kan gribes ind ved fejlagtige installationer eller andre udfordringer?
- Har enheden systemer og komponenter, som er forældede og derfor bør udskiftes først?
- Kan enheden beskytte forældede aktiver indtil udskiftning er muligt, fx via segmentering, således kompromittering formindskes?
- Hvordan vil fejlagtig opdatering eller installation af firmware påvirke enhedens drift?
- Er der kendte trusler og sårbarheder i sektoren eller i de aktiver enheden anvender, og hvordan holder enheden sig opdateret?

3.6 Effektivitet af foranstaltninger

Enheden bør med jævne mellemrum foretage tests og vurderinger af egen cybersikkerhed for at vurdere effektiviteten af deres foranstaltninger. Der findes ikke én korrekt test eller vurderingsmetode, men der er forskellige tests, som bør anvendes til forskellige formål. Miljøstyren anbefaler derfor, at vand- og spildevandsforsyninger anvender et flertal af tests og vurderingsmetoder til evaluering af forskellige facetter af enhedens samlede net- og informationssystemssikkerhed.

Udvalgte tests kan kræve teknisk viden og erfaring, og kan derfor udføres af eksterne tredjeparter. Enheden bør dog overholde egne forsyningskædesikkerhedsforanstaltninger ved eventuel anvendelse af tredjepart:

Relevante tests og vurderingsmetoder kan inkludere, men er ikke begrænset til
- Penetrationstests af enhedens digitale forsvar, for at identificere ukendte sårbarheder
- Test af logning, detektionsmetoder og hændelseshåndtering
- Aktivfortegnelser, konfigurations- og arkitekturgennemgange
- Sårbarhedshåndtering baseret på leverandørinformation og scanninger, heraf bl.a. passive scanninger
- Test af enhedens overgang til ødrift og manuel drift, enhedens *backup and restore*-protokoller samt komponentudskiftning fra nødlager

3.7 Cyberhygiejne og cybersikkerhedsuddannelse

Miljøstyrelsen anbefaler, at enheden anvender segmenteringslogikker til enhedens netværk på grund af dets fordelagtige anvendelse i vandsektoren, med henblik på beskyttelse af OT-system.

Alle fremhævede sikkerhedsstandarder i afsnit 2.*3 Sikkerhedsstandarder som Miljøstyrelsen anbefaler*, anvender segmenteringslogik i varierende grad. Ønsker vand- og spildevandsforsyningsenheden en isoleret segmenteringslogik, anbefaler Miljøstyrelsen anvendelsen af Purdue-modellen.

Disse vejledninger fra Sikkerdigital.dk er nyttige til generisk-god cybersikkerhedspraksis:
- Syv råd om it-sikkerhed
- OT-sikkerhed: 10 råd til beskyttelse af det fysiske produktionsapparat

Yderligere, er SektorCERTs 25 anbefalinger anvendelige til god cybersikkerhedspraksis i vandsektoren. SektorCERT er ikke en myndighed, men en non-profit forening med erfaring inden for cybersikkerhed i infrastruktur.

3.8 Kryptografi

Enheden bør mindst kryptere udvalgt information, som – hvis den kompromitteres, kan medføre betydelig skade for vand- eller spildevandsforsyningens drift eller overholdelse af lovgivning såsom GDPR.

Anvendes kryptografi i forbindelse med ældre produktionssystemskomponenter, såsom ældre PLC'er der ikke kan benytte moderne krypteringsmekanismer, kan kryptografi agere kompenserende ved at kryptere andet relevant information. Eksempelvis, kan enheden anvende kryptering i forbindelse med produktionsrelaterede adgangskoder og konfigurationsfiler i centrale systemer, eller produktionssystemsdatabaser og administrationsværktøjer.

Enheden bør derfor, ud over kryptering af information, også anse kryptering som en del af enhedens lagdelte forsvarsmekanismer, der bliver relevant for cyberbeskyttelse, når eksisterende cyberforsvar, såsom autentificering eller segmentering, har fejlet. Enheden bør derfor risikovurdere behovet for kryptering i samspil med vurderingen af øvrige foranstaltninger.

3.9 Personalesikkerhed, adgangskontrolpolitikker og forvaltninger af aktiver

Miljøstyrelsen anbefaler, at enheden ved formulering af adgangskontrolpolitik, tager udgangspunkt i egen risikoanalyse, således at adgang til enhedens net- og informationssystem tildeles på baggrund af vurdering af risiko – og konsekvenserne heraf. Miljøstyrelsen anbefaler, at enhedens adgangskontrolpolitik formuleres strammere ved adgang til aktiver af højere risiko- og konsekvensmæssig værdi.

Derudover, bør enheden inkludere fysisk miljø ved formuleringen af adgangskontrolpolitikker, da højt cybersikkerhedsniveau i vandsektoren praktisk kan inkludere adgangskontrol af OT-system med udgangspunkt i digitalisering af produktionsforanstaltninger.

Miljøstyrelsen anbefaler derfor, at enheden ved segmentering af net- og informationssystemer skaber overblik over eget fysiske miljø, og segmenterer det via adgangskontrol. Trods potentielt overlap med CER-lovens krav om fysisk sikkerhed, kan dette være behjælpeligt med henhold til NIS 2-loven, da adgang til enhedens net- og informationssystemer i visse tilfælde kan tilgås fysisk, såsom via produktionsforanstaltninger, og adgangskontrol på enkelt aktivniveau kan i nogle tilfælde afføde uhensigtsmæssige konsekvenser som kan vurderes uacceptable jf. NIS 2-politikker for risikostyring og informationssikkerhed.

Enhedens adgangskontrolpolitik og forvaltning af aktiver kan derfor formuleres i samspil med CER-lovens §9, nr. 2, såfremt enheden vurderer det fordelagtigt, at implementere personalesikkerhed og adgangskontrol i samspil med CER-lovens krav om baggrundskontrol.

3.10 Multifaktorautentificeringssystemer og nødkommunikationssystemer

Miljøstyrelsen anbefaler, at enheder overvejer multiautentificeringssystemer (MFA) som kompenserende sikkerhedsforanstaltning ved vedligeholdelse af ældre produkter, som ikke længere supporteres af udbyder (foranstaltning 5. Erhvervelse, udvikling og vedligeholdelse). Multifaktorautentificeringssystemer er velegnede til formålet, da adgang kan begrænses og derved mulighed for at udnytte sårbarheder. Dog, bør enheder som anvender MFA sådan, være opmærksomme på, at MFA ikke nødvendigvis beskytter mod alle de trusler som et usupporteret produkts udbydere tidligere har beskyttet mod. Derfor er denne løsning ikke nødvendigvis fyldestgørende for sikkerhedsmæssig vedligeholdelse af forældede produkter.

Enheden bør dog ikke udelukkende anvende MFA som kompenserende sikkerhedsforanstaltning. Miljøstyrelsen anbefaler, at enheden anvender MFA på alle relevante systemer i enhedens net- og informationssystem.

Enheden bør ved implementering af nødkommunikationssystemer prioritere intern nødkommunikation til formålet at opretholde samfundskritisk tjeneste og drift, samt nødkommunikation til relevante parter i enhedens beredskabs- og krisestyringsplaner.

Bilag A: Liste over relevante afsnit i CIS Controls

TABEL 1. Liste over relevante afsnit i CIS Controls

Foranstaltning	CIS Control
Politik for risikostyring og informationssikkerhed	
A. POLITIK FOR INFORMATIONSSIKKERHED	12.1, 12.2, 12.3, 12.4
B. POLITIK FOR RISIKOSTYRING	
Håndtering af hændelser	
A. HÅNDTERING AF HÆNDELSER	
B. LOGNING OG MONITORERING	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 8.11, 8.12
DRIFTSKONTINUITET	
A. DRIFTSKONTINUITET	
B. BACKUP	11.1, 11.2, 11.3, 11.4, 11.5
C. REDUNDANS	
D. KRISESTYRING	17.1, 17.2, 17.3, 17.4, 17.5, 17.9
FORSYNINGSKÆÆDESIKKERHED	15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7, 16.4, 16.5,
ERHVERVELSE, UDVIKLING OG VEDLIGEHOLDELSE	
A. ERHVERVELSE, UDVIKLING OG VEDLIGE-HOLDELSE	2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 4.8, 4.9, 4.10, 4.11, 4.12, 16.1, 16.2, 16.3, 16.12
B. HÅNDTERING AF SÅRBARHEDER	7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 16.6, 16.7,
EFFEKTIVITET AF FORANSTALTNINGER	
A. VURDERING AF EFFEKTIVITETEN AF DE IMPLEMENTEREDE FORANSTALTNINGER	17.7, 17.8, 18.3, 18.4
B. TEKNISKE TESTS	16.13, 16.14, 18.1, 18.2, 18.5
CYBERHYGIENE OG CYBERUDANNELSE	
A. CYBERHYGIEJNEPRAKSISSER	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 12.8, 16.8, 16.9, 16.10, 16.11,
B. CYBERSIKKERHEDSUDDANNELSER	14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8, 14.9
KRYPTOGRAFI	3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14
PERSONALESIKKERHED, ADGANGSKONTROLPOLI-TIKKER OG FORVALTNING AF AKTIVER	
A. PERSONALESIKKERHED	
B. ADGANGSKONTROL	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 12.5, 12.6, 12.7,

C. FORVALTNING AF AKTIVER	1.1, 1.2, 1.3, 1.4, 1.5, 13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8, 13.9, 13.10, 13.11
MULTIFAKTORAUTENTIFICERING OG NØDKOMMUNIKATIONSSYSTEMER	
A. MULTIFAKTORAUTENTIFICERING	
B. NØDKOMMUNIKATIONSSYSTEMER	17.6, 17.7,

Resume

Forsyningsselskaber som er omfattede af NIS 2-loven skal leve op til NIS 2-lovens §6. *Foranstaltninger til styring af cybersikkerhedsrisici,* som pålægger forsyningers net- og informationssystemer krav om tekniske, operationelle og organisatoriske foranstaltninger. Miljøstyrelsen har skrevet en vejledning, som skal hjælpe NIS 2-omfattede vand- og spildevandsforsyninger med foranstaltningsimplementering.

Vejledningen tager afsæt i vandsektorens særlige kendetegn, levering af tjeneste, og hjælper ved at angive sektorspecifikke anbefalinger og fremhæve relevante overvejelser i forbindelse med NIS 2-lovens krav om foranstaltninger.

Miljøstyrelsen
Lerchesgade 35
5000 Odense C

www.mst.dk