Cybersikkerhed i vandsektoren i Nordtyskland og Syddanmark

NEPTUN wird finanziert von Interreg Deutschland-Dänemark mit Mitteln aus dem Europäischen Fond für Regionalentwicklung. Lesen Sie mehr über Interreg Deutschland-Dänemark auf www.interreg5a.eu

Indholdsfortegnelse

Indledning

EU står overfor en forværret sikkerhedspolitisk situation, og cyberrobusthed i kritisk infrastruktur har fået større opmærksomhed.

Det kan have ødelæggende og vidtrækkende konsekvenser for forsyningssikkerheden, sundhed, miljø og økonomi, hvis kriminelle eller fjendtlige grupper får held med at hacke kritisk infrastruktur som vandforsyning og spildevandshåndtering. En genetablering af IT-systemer kan desuden være både omkostningstungt og tidskrævende.

Truslen betyder, at vandselskaber på begge sider af den dansk-tyske grænse retter fokus mod cybersikkerhed og skruer op for investeringer heri. Leverandører, der tilbyder løsninger hertil, har således en unik mulighed for at få fodfæste på et nyt marked.

En vellykket ekspansion kræver imidlertid indsigt og viden, som denne rapport sigter på at give leverandører, der overvejer at udvide deres aktiviteter til vandsektoren i Danmark hhv. Tyskland.

Rapporten er udarbejdet af Dansk Brand- og Sikringsteknisk Institut, PDV Systeme GmbH og SDU.

Det skal bemærkes, at det ikke har været muligt at finde data specifikt for Interreg programregionen, dvs. data for Danmark og Tyskland benyttes i stedet for.

Betegnelserne ”vandsektor” og ”vandselskaber” bruges som en fællesbetegnelse vandforsynings- og spildevandssektoren hhv. for selskaber i de to sektorer.

Marts 2023.

Vandforsynings- og spildevandsselskaber i Danmark

Der er ca. 2.600 almene vandforsyningsselskaber i Danmark, og de leverer drikkevand til ca. 97% af den danske befolkning (Miljøministeriet, 2022).

Langt størstedelen er privatejede (fortrinsvis forbrugerejede); alene 87 er kommunalt ejede. Det høje antal almene vandforsyningsselskaber skyldes, at der i landdistrikter har været tradition for at etablere forbrugerejede vandværker i lokale fællesskaber (Miljøministeriet, 2022).

De almene vandforsyningsselskaber varierer betydeligt i størrelse – fra at levere vand til flere hundrede tusinde borgere til at levere drikkevand til så få som 10 ejendomme (Miljøministeriet, 2022A).

Ca. 40 af de almene vandforsyningsselskaber leverer udover vand også f.eks. el, gas og fjernvarme; de betegnes som multiforsyningsselskaber (Deloitte og Miljøstyrelsen, 2022).

Den resterende del af befolkningen (3%) modtager drikkevand fra ca. 50.000 små ikke-almene vandforsyninger, der forsyner færre end 10 ejendomme – ofte er der tale om en brønd eller boring, der kun forsyner en enkelt husstand (Miljøministeriet, 2022A).

På trods af det beskedne antal kommunalt ejede vandforsyningsselskaber, står de for ca. to tredjedele af den samlede produktion af drikkevand (Miljøministeriet, 2022).

Der er ca. 1.000 rensningsanlæg i Danmark, hvoraf ca. 800 er kommunalt ejede, herunder et mindre antal fælleskommunale, imens de resterende 200 rensningsanlæg er i privat ejerskab. De kommunalt ejede rensningsanlæg drives af spildevandsselskaber, hvoraf der er ca. 100, svarende til en pr. kommune (Miljøministeriet, 2022).

Antallet af rensningsanlæg er reduceret betydeligt i de senere år. Det skyldes, at flere små og lavteknologiske rensningsanlæg er nedlagt til fordel for større og mere avancerede. De 300 største og mest avancerede anlæg står således i dag for rensningen af 90% af det danske spildevand. Samme udvikling har ikke fundet sted hos vandforsyningsselskaber (Deloitte og Miljøministeriet, 2022).

Både vandforsyningsselskaber og spildevandsselskaber er i Vandsektorloven underlagt et ”hvile-i-sig-selv”-princip. Det betyder, at der over en årrække skal være balance imellem indtægter og udgifter. Vandselskaberne er 100% taktfinansierede, dvs. den daglige drift og investeringer betales fuldt ud af kunderne (DANVA, 2022).

Vandselskaber med en årlig debiteret vandmængde over 200.000 m3 eller kommunale vandselskaber er også underlagt indtægtsrammer, der sætter et årligt loft over indtægter og indeholder effektiviseringskrav. Indtægtsrammen fastsættes ud fra det enkelte vandselskabs omkostninger til drift, vedligehold, investeringer, finansielle omkostninger og ikke-påvirkelige omkostninger såsom skatter og afgifter (Konkurrence- og forbrugerstyrelsen, 2019).

Indtægtsrammerne skal sikre at:

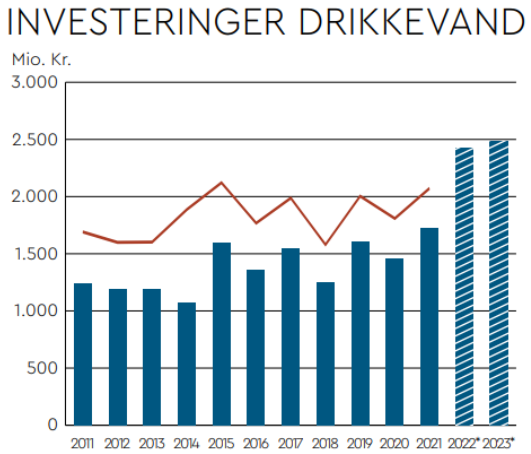
- *”Forbrugere og virksomheder ikke betaler for meget for vand og spildevand.*
- *Selskaberne har tilstrækkelige midler til at drive, vedligeholde og udvikle deres infrastruktur for at sikre fortsat høj kvalitet og forsyningssikkerhed.*
- *Selskaberne løbende effektiviserer deres drift og anlæg i takt med produktivitetsudviklingen i resten af den danske økonomi”* (Konkurrence- og forbrugerstyrelsen, 2022).

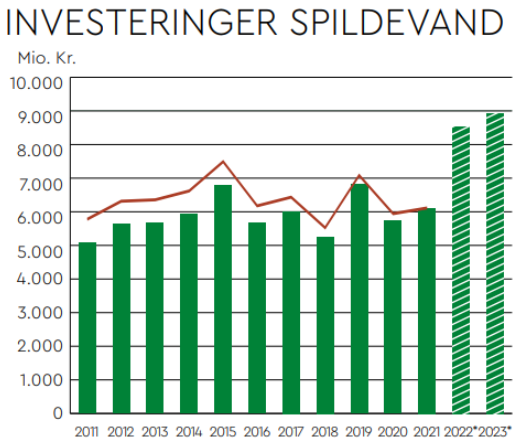
Mindre forbrugerejede vandselskaber med en årlig debiteret vandmængde mellem 200.000 – 800.00 m3 vand har siden 1. januar 2020 kunnet udtræde af indtægtsrammerne. De er dog fortsat underlagt "hvile-i-sig-selv"-princippet (Konkurrence- og forbrugerstyrelsen, 2022).

Vandselskaberne har været dygtig til at høste let opnåelige effektiviseringsgevinster og innovationsløsninger, og de har ofte været foran myndighedernes effektiviseringskrav. Sektoren har dog tiltagende svært ved at holde tempo, og den nuværende regulering anses af brancheorganisationer som utidssvarende i forhold til at balancere reinvesteringer og investeringer i nye løsninger (DANVA, 2022). Vandsektorloven er pt. under revision, og et forslag til en ny vandsektorlov blev sendt i høring medio 2022 (PwC, 2022).

Brancheaktører forventer, at investeringsniveauet hos vandselskaber i Danmark vil stige betydeligt i de kommende år, herunder illustreret af brancheorganisationen Danva for drikkevands- og spildevandselskaber, som er omfattet af vandsektorloven, og som har en debiteret vandmængde over 800.000 m3 årligt (DANVA, 2022).

Grafik 1: Investeringer i drikkevand og spildevand for selskaber omfattet af vandesektorloven med en debiteret årlig vandmængde over 800.000 m3.





Kilde: Vand i tal 2022, DANVA, side 15.

Vandforsynings- og spildevandsselskaber i Tyskland

Det er ca. 5.800 vandforsyningsselskaber i Tyskland, hvoraf ca. 1.600 selskaber står for 80% af den samlede produktion af drikkevand. Tilsvarende er der i niveauet 6.500 spildevandsselskaber i Tyskland (Arbeitsgemeinschaft Trinkwassertalsperren et al., 2020).

Vandforsyning og spildevand er kommunale kerneopgaver, dvs. kommunerne skal sikre forsyning af drikkevand i høj kvalitet, og de skal bortskaffe og håndtere spildevand på forsvarlig vis (Arbeitsgemeinschaft Trinkwassertalsperren et al., 2020).

Kommunerne kan vælge at håndtere opgaverne i et rent offentligt setup eller i samarbejde med private aktører. Vælger en kommune at samarbejde med private aktører er det fortsat kommunen, der har det ultimative ansvar for forsyningssikkerheden og kvaliteten, ligesom kommunen som oftest også har den bestemmende indflydelse i samarbejdet. Kommunerne har derudover mulighed for at indgå i tværkommunale sammenslutninger for at opnå stordrifts- og effektiviseringsfordele (Arbeitsgemeinschaft Trinkwassertalsperren et al., 2020).

I 2018 var vandforsyning primært organiseret i offentlig regi (67%), mens selve produktionen af drikkevand fordelte sig med 43% på offentlige organisationsformer og 57% på offentlig-private organisationsformer (Arbeitsgemeinschaft Trinkwassertalsperren et al., 2020).

Spildevand håndteres næsten udelukkende i offentlig regi. I 2014 viste en undersøgelse fra Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA), at ca. 95% af alt spildevand håndteres af kommunerne (Arbeitsgemeinschaft Trinkwassertalsperren et al., 2020).

Prisen på drikkevand og spildevand fastsættes af byrådene, når opgaven løses i offentlig regi, og i virksomhedernes bestyrelse, når opgaven løses i samarbejde med private aktører. Lovgivning på kommunalt- og delstatsniveau udstikker en ramme for priskalkulationen, men dikterer ikke beregningen. Myndighederne fører tæt kontrol med priserne (Arbeitsgemeinschaft Trinkwassertalsperren et al., 2020).

Prisdannelsen skal være gennemsigtig og tilgængelig for offentligheden og følge tre principper:

1. ”Äquivalenzprinzip”; der skal være et passende forhold mellem leveret ydelse og betaling.

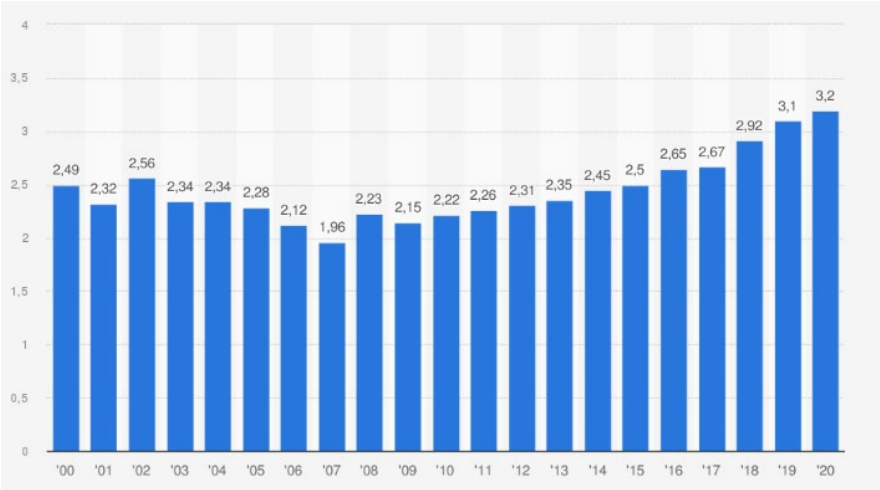
2. ”Kostendeckungsprinzip”; betalingen for en ydelse skal dække, men ikke overstige, omkostningerne forbundet med ydelsen.

3. ”Gleichbehandlungsprinzip”; forskelsbehandling af individer eller grupper af kunder er ikke tilladt.

(Bundesverband der Energie- und Wasserwirtschaft e.V., Verband Kommunaler Unternehmen e.V. (2012), (Arbeitsgemeinschaft Trinkwassertalsperren et al., 2020).

Investeringsniveauet blandt vandselskaber i Tyskland har været stigende i flere år, se grafik 2 næste side, der viser investeringer i offentlig vandforsyning (Bundesverband der Energie- und Wasserwirtschaft (BDEW), 2020). Stigningen er et udtryk for, at vandselskaberne i stigende grad skal håndtere udfordringer, der knytter sig til f.eks. kvalitet, infrastruktur, klima og demografi (Arbeitsgemeinschaft Trinkwassertalsperren et al., 2020).

Grafik 2: Investeringsniveau i offentlig vandforsyning i Tyskland fra 2000 til 2020, i mia. EUR



Kilde: Statista, 2022 på baggrund af data fra BDEW.

EU-lovgivning

I november 2022 vedtog EU-Parlamentet NIS2-direktivet, der indfører nye og væsentlige regler for cybersikkerhed i den private og offentlige sektor i EU. NIS2-direktivet afløser NIS1-direktivet fra 2016 (Horten, 2022).

NIS2 afventer nu endelig vedtagelse i Det Europæiske Råd, men skal være implementeret i medlemsstaternes nationale lovgivning senest 21 måneder efter direktivet træder i kraft, forventeligt senest i efteråret 2024. Begge direktiver er minimumsharmoniseringsdirektiver, der betyder, at medlemsstaterne gerne må vedtage lovgivning, der sikrer et højere niveau af cybersikkerhed, end direktiverne foreskriver (Horten, 2022).

Danmark og Tyskland har igangsat arbejdet med at implementere NIS2 i national lovgivning, men hvordan det konkret udmønter sig er endnu uklart. Herunder følger en beskrivelse af de rammer, som NIS2 udstikker for medlemsstaternes fremtidige lovgivning.

NIS står for Net- og Informationssystemer, dvs.:
- kommunikationsnet
- forbundne anordninger, der via et program udfører automatisk behandling af digital data
- digital data, der lagres, behandles, fremfindes eller overføres (Storgaard, 2022).

Formålet med NIS2 er at styrke og ensarte cybersikkerhed hos virksomheder, organisationer og institutioner, der tilhører sektorer, som anses for samfundskritisk hhv. kritisk for økonomien (Horten, 2022). Der er tale om 15 sektorer, heriblandt vandforsyning og spildevand. Spildevand var ikke omfattet af NIS1, dvs. der er tale om en tilføjelse i NIS2. Organisationer i de 15 sektorer kaldes ”væsentlige enheder” (f.eks. organisationer i vandforsyningssektoren) eller ”vigtige enheder” (f.eks. organisationer i spildevandssektoren) (Horten, 2022).

Direktivet omfatter private virksomheder samt offentlige organisationer på regionalt og statsligt niveau. Det er op til medlemsstaterne, om direktivet også skal gælde på kommunalt niveau (Bisgaard, 2022).

Virksomheder med færre end 50 ansatte og en årlig omsætning eller en årlig balance på under 10 mio. EUR, er som udgangspunkt ikke omfattet af NIS2. Der er dog undtagelser, hvis der er tale om *”enheder, der leverer ydelser der er kritiske for samfundet, offentligheden eller en konkret sektor”* (Horten, 2022).

Men, hvad står der i NIS1 og NIS2? Begge direktiver indeholder krav rettet mod medlemsstaterne og mod virksomheder, organisationer og institutioner i sektorerne. I direktiverne pålægges sidstnævnte gruppe ”*at træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre sikkerhedsrisici og begrænse skaderne i tilfælde af en sikkerhedshændelse*” (Horten, 2022).

I NIS1 var det i høj grad op til medlemsstaterne at definere, hvordan det skulle gøres, men i NIS2 forpligtes virksomheder, organisationer og institutioner til at opfylde konkrete minimumskrav (Verband Kommunaler Unternehmen, 2022). Der er tale om:

- *”Politikker for risikoanalyse og informationssikkerhed*
- *Håndtering af hændelser*
- *Driftskontinuitet og krisestyring (back-up mv.)*
- *Forsyningskædesikkerhed, herunder leverandørstyring/-sikkerhed*

- *Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer*
- *Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici*
- *Retningslinjer for basal "computer hygiejne" og træning i cybersikkerhed*
- *Politikker for brug af kryptografi og kryptering*
- *Medarbejdersikkerhed, adgangskontrol og asset management*
- *Sikring af interne kommunikationssystemer"* (Horten, 2022).

I NIS1 var der krav om oprettelsen af Computer Incident Response Teams (CSIRIT), der skal informeres om væsentlige "hændelser". En væsentlig hændelse er, *" […] hvis hændelsen eller cybertruslen (i) har forårsaget eller potentielt kan forårsage væsentlige leverings- eller driftsforstyrrelser eller økonomiske tab for enheden, eller (ii) hændelsen har påvirket eller kan påvirke andre fysiske eller juridiske personer ved at forårsage betydelige materielle eller immaterielle tab*" (Horten, 2022). I Danmark er Center for Cybersikkerhed (CFCS) udpeget som CSIRIT (Horten, 2022), i Tyskland varetages rollen af Bundesamt für Sicherheit in der Informationstechnik (BSI) (BSI, 2022b).

I NIS2 udvides informationspligten, så væsentlige hændelser nu skal indrapporteres indenfor 24 timer, og hændelserne skal under visse omstændigheder også meddeles tredje part som f.eks. kunder (Verband Kommunaler Unternehmen, 2022).

I NIS1 var det alene den juridiske enhed f.eks. virksomheden, der var ansvarlig for overholdelsen af direktivet. I NIS2 kan ledelsen også drages til ansvar. Ledelsen skal*: " […] godkende de risikohåndteringsforanstaltninger, som enheden træffer vedrørende cybersikkerhed og føre tilsyn med implementeringen og vedligeholdelsen heraf"* (Horten, 2022). Det er medlemsstaternes ansvar at sikre, at lederne regelmæssigt følger kurser for at opnå tilstrækkelig viden og færdigheder, der gør dem i stand til at forstå og vurdere risici og styringspraksisser – og hvordan disse påvirker den daglige drift (Bisgaard, 2022).

Medlemsstaternes myndigheder skal føre tilsyn med at bestemmelserne overholdes. I NIS2 skærpes pligten, idet der for væsentlige enheder (vandforsyning) skal føres proaktivt tilsyn og for vigtige enheder (spildevand) fortsat skal være opfølgende tilsyn. Der kan udstedes advarsler eller pålæg, og der kan uddeles bøder – for væsentlige enheder op til 10 mio. EUR eller 2% af virksomhedens globale omsætning og for vigtige enheder op til 7 mio. EUR eller 1,4% af virksomhedens globale omsætning (Horten, 2022).

Internationale standarder

Den internationale standardiseringsorganisation ISO Standards tilbyder certificeringer indenfor en lang række områder såsom certificeringer i cybersikkerhed. En ISO-certificering er internationalt anerkendt og udbredt i flere brancher – også i vandsektoren i Danmark og Tyskland. ISO-standarder med fokus på cybersikkerhed er primært ISO/EIC 27001, ISO/EIC 27002 og ISO/EIC 27005 (Mikkelsen, 2022). Standarderne har fokus på informationssikkerhed, hvor der bl.a. stilles krav til risikostyring, dokumentation af processer og fordeling af ansvar og roller for informationssikkerhed (Dansk Standard, 2023).

Tysk lovgivning og branchestandarder

NIS1 er implementeret i loven ”Gesetz zur Umsetzung der NIS-Richtlinie“ (BSI, 2023). Den udgør sammen med loven „IT-Sicherheitzgesetz 2.0” fra 2021 kernen i tysk lovgivning for cybersikkerhed (BSI, 2023c) (USD, 2023).

Tyskland har defineret ti sektorer med 29 underbrancher som kritisk infrastruktur. Der er tale om sektorer og brancher, hvor f.eks. afbrydelser eller nedbrud potentielt kan true forsyningen og den offentlige sikkerhed. Vandsektoren med vandforsyning og spildevand hører til kritisk infrastruktur (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2022).

Hvis leverandører i disse sektorer og underbrancher opfylder specifikke tærskelværdier, defineres de som ”kritiske leverandører”. For vandsektoren er det f.eks. en debiteret vandmængde på 22 mio. kubikmeter årligt og 500.000 indbyggere tilsluttet kanalisationssystem (OpenKRITIS, 2022). Dette gør sig dog alene gældende for ca. 50 ud af de i alt ca. 5.800 vandforsyningsselskaber i Tyskland (Neuerer, 2021).

Kritiske leverandører er underlagt en række krav, såsom at de skal:

- indberette brud på IT-sikkerheden til BSI
- tage passende organisatoriske og tekniske forholdsregler for at forhindre IT-sikkerhedsbrud, herunder skal de sikre, at deres IT-systemer er på et passende niveau
- hvert 2. år skal dokumentere overfor BSI, at deres IT-sikkerhed er på et passende niveau.

(BSI, 2022; OpenKRITIS, 2022).

Myndighederne har specificeret kravene til de kritiske leverandører i et katalog med mulige organisatoriske, tekniske samt afværge- og skadesbegrænsende tiltag (BSI, 2022a).

Brancheorganisationer i de ti sektorer har fulgt op med at udarbejde branchespecifikke sikkerhedsstandarder, som virksomheder kan følge for at leve op til lovgivningen (BSI, 2022). I vandsektoren er det organisationerne Deutscher Verein des Gas- und Wasserfaches (DVGW) og Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V. (DWA), som står bag sikkerhedsstandarderne. De to brancheorganisationer opfordrer stærkt til, at også ikke-kritiske leverandører, som minimum følger basisanbefalingerne i standarden (DVGV og DWA, 2022).

Dansk lovgivning og branchestandarder

I Danmark er NIS1 for vandsektoren implementeret i lovgivningen via en bekendtgørelse. Bekendtgørelsen har dog ikke ført til krav til sektoren (Deloitte og Miljøstyrelsen, 2022), da der i et bilag specificeres, at ingen vandforsyninger er omfattet af bekendtgørelsen (Retsinformation.dk, 2022).

Regeringen lancerede i december 2021 en ny national strategi for cyber- og informationssikkerhed for årene 2022-2024. I strategien udpeges drikkevand og spildevand som samfundsvigtige sektorer (Hansen, 2022).

Miljøministeriet er den ansvarlige myndighed for vand- og spildevandssektoren, og de pålægges i strategien bl.a. at udarbejde en sektorstrategi og handlingsplan for cyber- og informationssikkerheden i vandsektoren. I den forbindelse har Deloitte i samarbejde med Miljøministeriet gennemført en analyse af cyber- og informationssikkerheden i den danske vandsektor (Deloitte og Miljøministeriet, 2022).

Deloitte og Miljøstyrelsen vurderer i analysen, at minimum 90 vandforsyningsselskaber (primært de større med en årlig debiteret vandmængde på > 800.000 m3) og 100 spildevandsselskaber er samfundskritisk infrastruktur og vil være omfattet af den fremtidige cyber- og informationsstrategi for sektoren (Deloitte og Miljøministeriet, 2022), se tabel 1:

Tabel 1: Vurdering af, hvor mange vandselskaber, der bør indgå i den kritiske infrastruktur

Kategori	Kriterie (årlig debiteret vandmængde)	Antal selskaber	Kritisk infrastruktur
Multiforsyningsselskaber	>800.000 m3 og flere forsyningsarter	40	Alle
Store vandselskaber	>800.000 m3	50 + 100 spilde-vandsselskaber	Alle
Mellem vandselskaber	200.000-800.000 m3	150	En andel
Små vandselskaber	17.000-200.000 m3	1.200	Ingen / en mindre del
Mikro vandselskaber	<17.000 m3	450	Ingen

Kilde: Deloitte og Miljøministeriet, side 7 og 26.

Der findes to danske brancheorganisationer indenfor vandforsyning og spildevand – DANVA og Danske Vandværker. DANVA's medlemmer er primært større vandforsyningsselskaber og kommunale spildevandsselskaber, imens Danske Vandværkers medlemmer primært er små og mindre vandværker (Deloitte og Miljøministeriet, 2022).

Der findes ikke IT-branchestandarder for selskaber i vandsektoren.

DANVA anbefaler grundlæggende deres medlemmer at følge vejledninger og trusselsadvarsler fra CFCS samt følge statens tekniske minimumskrav for IT-sikkerhed (DANVA, 2022b). DANVA er desuden fra januar 2023 medlem af EnergiCert, en brancheorganisation for virksomheder indenfor kritisk infrastruktur, der hjælper deres medlemmer med at overvåge cybertrusler og håndtere cyberangreb (DANVA, 2022b; EnergiCert, 2022).

Derudover tilbyder både DANVA og Danske Vandværker deres medlemmer forskellige råd, vejledninger, netværk, forsikringer og services etc. indenfor cybersikkerhed.

Modenhedsniveau af tyske vandselskaber

Tyske vandselskaber har i de senere år i stigende grad prioriteret cybersikkerhed, og sektorens virksomheder anvender generelt en bred vifte af tiltag til at forebygge, afværge, håndtere og inddæmme cyberangreb.

Udviklingen har været drevet af:

- øgede krav i form af lovgivning, regulering og delvis påkrævede interne auditeringer
- større bevågenhed og kontrol fra myndighederne side
- branchefokus, herunder udviklingen af standarder og værktøjer fra brancheorganisationer.

Vandselskabernes arbejde med cybersikkerhed har således været hjulpet af, at de har følt en vis nødvendighed, samt at de har haft en ramme for og værktøjer til at arbejde med temaet og ikke mindst, at de har haft partnere, de har kunnet søge hjælp og rådgivning hos.

For en stor del af vandselskaberne er cybersikkerhed dog ikke et nemt tilgængeligt område. I en undersøgelse fra brancheorganisationer DWA og DVGW fra 2021 svarede beskedne 12% af de 60 adspurgte vandselskaber, at de vurderede deres kompetencer indenfor cybersikkerhed som værende ”gode”, imens resten af besvarelserne fordelte sig ligeligt på ”middel” og ”dårlig”. Færre end 20% af de adspurgte vandselskaber havde nogensinde foretaget en risikoanalyse af deres IT-systemer (KWB, 2022).

I modsætning til de større vandselskaber, mangler små vandselskaber ofte forståelse for cybersikkerhed, har begrænsede midler og budget hertil, ligesom de ikke altid har de rette faglige kompetencer. Cybersikkerhed kan synes som en vanskelig opgave, der kommer oven i den daglige drift, som til en hver tid har 1. prioritet. Mange små vandselskaber indkøber ekstern ekspertise til at løfte opgaven, men risikerer, uden tilstrækkelig forståelse og viden, at købe løsninger i blinde.

Nogle vandselskaber håndterer usikkerheden ved konsekvent at holde sig til f.eks. branchestandarder. Dette kan i værste fald blive så rigidt og ufleksibelt, at de løsninger, der vælges og implementeres, ikke passer til de måske særlige behov eller den unikke situation vandselskabet måtte have.

Modenhedsniveau af danske vandselskaber

Vandselskaber i Danmark har igennem flere år haft cybersikkerhed på dagsordenen. En større del af virksomhederne i sektoren har således implementeret forskellige tiltag, såsom IT-sikkerhedspolitikker, uddannelse og arbejdet med awareness (Deloitte og Miljøministeriet, 2022).

Niveauet for cybersikkerhed er dog højest hos de større vandselskaber og falder i takt med selskabernes størrelse (Deloitte og Miljøministeriet, 2022).

De mindre og mellemstore vandselskaber drives af ansatte, der har fokus på og er dygtige til drift og udvikling af kerneopgaven, men som ofte mangler viden om og forståelse for cybersikkerhed. De har begrænsede økonomiske ressourcer, og især de mindre vandselskaber drives ofte på frivillig basis eller af deltids- eller timeansatte, dvs. de er pressede på kompetencer, tid såvel som midler, når det kommer til cybersikkerhed.

I Deloitte og Miljøministeriets undersøgelse af cyber- og IT-sikkerheden i den danske vandsektor fremgår det f.eks. også at langt størstedelen af de mindre vandselskaber ikke eller kun i delvist omfang har en dokumenteret IT-sikkerhedspolitik (Deloitte og Miljøministeriet, 2022).

De mindre og mellemstore vandselskaber kan løse udfordringen ved at outsource cybersikkerhed til eksterne samarbejdspartnere, der har de nødvendige fagspecifikke kompetencer. Der er dog en reel risiko for, at vandselskaberne, fordi de mangler forståelse for samt viden og kompetencer om emnet, ender med at købe løsninger, der ikke passer til deres behov. De forstår f.eks. ikke i tilstrækkelig grad, hvordan deres IT-systemer og anlæg er forbundne, hvor og hvorfor de er sårbare overfor cyberangreb, hvilke trusler de skal tage højde for og hvilke IT-løsninger, der findes på markedet.

Forsyningssikkerheden afhænger i høj grad af, om vandselskaberne i tilfælde af nedbrud kan drifte anlæggene manuelt – og et argument blandt (især små) vandselskaber, hvorfor cybersikkerhed ikke er helt så væsentlig at fokusere på, er, at de altid har mulighed for at drifte eller stoppe anlæggene manuelt, skulle det blive nødvendigt.

Deloitte og Miljøministeriets undersøgelse viser dog, at en betydelig del af vandselskaberne – små som store - ikke tester eller kun delvist tester evnen til at kunne køre manuel drift – dvs. hvorvidt det reelt kan lade sig gøre er uvist (Deloitte og Miljøministeriet, 2022).

Undersøgelsen peger også på, at store multiforsyningsselskaber primært har fokus på cybersikkerhed indenfor energi. Både vand og energi er defineret som kritisk infrastruktur. I modsætning til vandsektoren, er cybersikkerhed i energisektoren dog underlagt regulering, lovkrav og standarder. At forhøje niveauet af cybersikkerhed er omkostningstungt, så vand inkluderes ofte kun i tiltag, når der er overlap til områder, hvor multiforsyningsselskaberne er lovmæssig forpligtede. Miljøministeriet og Deloitte understreger, at en øget centralisering og standardisering i sektoren er en nødvendighed, hvis virksomhedernes samlede niveau skal løftes (Deloitte og Miljøministeriet, 2022).

Aktuelle udfordringer vedr. cybersikkerhed i vandsektoren

IT-trusselsbilledet overvåges i Danmark af CFCS og i Tyskland af BSI. De to myndigheder udsender advarsler, hvis det er nødvendigt, ligesom de løbende udarbejder analyser på lande- og delvist også brancheniveau.

Vandsektoren indgår i CFCS' landsdækkende trusselsvurdering for Danmark. Vurderingen tager udgangspunkt i fem mulige trusler:

1. Cyberspionage, hvor f.eks. fremmede stater stjæler viden og data for at fremme egne interesser. CFCS vurderer pt. truslen herfra som meget høj, dvs. angreb er meget sandsynlig.
2. Cyberkriminalitet, hvor hackere via tyveri, bedrageri eller afpresning beriger sig økonomisk. CFCS vurderer pt. truslen herfra som meget høj, dvs. angreb er meget sandsynlig.
3. Cyberaktivisme, hvor individer eller grupper udfører cyberangreb for at få opmærksomhed til deres dagsorden eller for at straffe. CFCS vurderer pt. truslen herfra som høj, dvs. angreb er sandsynlig.
4. Destruktive cyberangreb, hvor angreb betyder død, personskade, betydelig skade på fysiske objekter og ødelæggelse og forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning. CFCS vurderer truslen herfra som lav, dvs. angreb er mindre sandsynlig.
5. Cyberterrror, hvor angreb forvolder fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur. CFCS vurderer truslen herfra som ingen, dvs. angreb er usandsynlig (CFCS, 2022d).

Deloitte og Miljøstyrelsen vurderer i deres undersøgelse, at den mest overhængende trussel mod den danske vandsektor er destruktive angreb, dvs. angreb hvor der manipuleres eller slukkes for anlæg, så forsyningen eller kvaliteten trues (Deloitte og Miljøstyrelsen, 2022).

Destruktive cyberangreb imod vandselskaber kan f.eks. være at ændre/ stoppe tilførslen af kemikalier, så der er risiko for sundhed og miljø, eller ved at øge trykket i vandrør, så disse sprænges og ødelægges.

Vandselskaberne har dog ofte backup-planer og/ eller kan modtage vand fra andre vandselskaber, så vandkvaliteten ikke bringes i fare. Overordnet set vurderer Deloitte og Miljøstyrelsen truslen imod vandselskabers anlæg som lav (Deloitte og Miljøstyrelsen, 2022).

EnergiCert vurderer tilsvarende, at der er risiko for fjendtlige cyberaktiviteter, men ikke risiko for aktiviteter, der kan påvirke kritisk dansk infrastruktur. De vurderer, at mange selskaber i forsyningssektoren har en god beskyttelse i forhold til de nuværende angrebsmetoder, så risikoen for, at kontrolsystemer bliver ramt, er lav (EnergiCert, 2022a).

BSI peger på ransomware som den primære cybertrussel mod tyske virksomheder. Ransomware er software, der blokerer for adgangen til computere eller data ved hjælp af kryptering. Ofte forlanger hackerne en løsesum for at fjerne blokeringen, og hvis ikke løsesummen betales, trues der med at ødelægge eller videresælge data. BSI vurderer, at ransomware angreb er professionaliseret i de senere år, hvor angreb udføres af flere hackergrupper i fællesskab. Der er nærmest opstået en form for værdikæde, hvor delopgaver i angrebene outsources til specialiserede grupper. BSI vurderer, at hackere har relativ let adgang til tyske virksomheders IT-systemer, da deres servere ofte er usikre, åbne eller direkte fejlkonfigurerede, hvilket åbner op for en bred angrebsflade (BSI, 2022).

BSI vurderer konkret, at vandsektoren især har mangler i forhold til deres ISMS- systemer. ISMS står for Informations Security Management Systems og dækker over, hvordan en

organisation definerer, dokumenterer og driver forskellige foranstaltninger for at sikre og beskytte sine informationer og aktiver mod trusler og sårbarheder (BSI, 2022).

Opgørelser fra EnergiCert og BSI tegner et billede af en dansk og tysk energi- og forsyningssektor, der oplever et stigende antal cyberangreb. EnergiCert har registeret 48 succesfulde cyberangreb (dvs. angreb, der er kommet forbi forsvarsmekanismer og har udrettet betydelig skade) indenfor energi- og forsyningssektoren i Europa siden 2015, hvoraf 22 har fundet sted i 2022. Flest angreb fandt sted i Tyskland (12 angreb) og næstflest angreb fandt sted i Danmark (6 angreb) (EnergiCert, 2022a). Tilsvarende fik BSI i 2022 meldinger om 10 IT-sikkerhedsbrud hos kritiske leverandører i vandforsyningssektoren (BSI, 2022).

En af grundene til det stigende antal cyberangreb i vandsektoren er formentlig den anspændte sikkerhedspolitiske situation i Europa som følge af Ruslands angrebskrig mod Ukraine. Danmark og Tyskland risikerer med deres støtte til Ukraine at blive opfattet som en fjendtligsindet stat og dermed blive mål for hybrid krigsførelse, hvor ukonventionelle metoder som f.eks. cyberangreb mod kritisk infrastruktur sættes ind for at lamme eller skade samfund.

Der er dog formodentlig et stort ”mørketal” i offentliggørelsen af cyberangreb i vandsektoren. Cyberangreb findes i forskellige udformninger og med forskellige niveauer af sikkerhedsbrud. Angreb, der afværges registres eller offentliggøres ikke, ligesom cyberangreb, hvor der ikke vurderes at være sket skade, ofte ej heller kommer offentligheden til kendskab. Derudover er der cyberangreb som aldrig opdages – f.eks. angreb, hvor der ”brydes ind” og kopieres men ikke stjæles, eller angreb, hvor der installeres ”bagdøre” til senere indbrud.

Vandselskaberne er desuden tøvende med at delagtiggøre offentligheden i IT-sikkerhedsbrud - medmindre det er tvingende nødvendigt. IT-sikkerhedsbrud skaber naturligt nok stor utryghed hos forbrugere, virksomheder og myndigheder, ligesom vandselskaberne kan risikere, at der rejses tvivl om deres IT-sikkerhedssetup, -niveau og håndtering. Faren ved at holde kortene tæt til kroppen er dog, at sektoren ikke erfaringsudveksler, lærer af hinanden eller hjælper hinanden til at imødegå cybertrusler.

Markedet for cybersikkerhed i vandsektoren i Tyskland

EU-parlamentets vedtagelse af NIS2-direktivet har fået efterspørgslen efter cybersikkerhedsløsninger til at stige markant hos tyske virksomheder, og markedet for cybersikkerhed i Tyskland vurderes at kunne opnå tocifrede vækstrater i de kommende år.

Især kravet om "*Forsyningskædesikkerhed, herunder leverandørstyring/-sikkerhed"* har betydet, at flere virksomheder ser en nødvendighed i at beskæftige sig med cybersikkerhed. Efterspørgslen intensiveres af, at NIS2 senest skal være implementeret og dermed gældende i tysk lovgivning i efteråret 2024 – dvs. der er en relativ kort tidsfrist til at opfylde lovens krav.

Tyske virksomheder efterspørger indledningsvist ofte ikke tekniske løsninger, men snarere viden om og træning i cybersikkerhed. Et niveauløft af virksomheders cybersikkerhed kræver organisatorisk opmærksomhed og støtte men også allokering af tid og penge, hvilket virksomhederne i høj grad synes at være indstillede på og villige til.

Selvsamme billede gør sig gældende for virksomheder i den tyske vandsektor. Vandforsyning og spildevand er dog kommunale kerneopgaver, hvilket betyder, at indkøb af produkter og ydelser over et vist beløb skal i udbud. Kommunerne hyrer ofte konsulentbureauer til at fastlægge kravspecifikationer og udarbejde udbudsmateriale, når de skal investere i cybersikkerhed. Udbuddene bliver ofte meget specifikke med megen lidt spillerum og prisen hurtigt den afgørende faktor, når kommuner skal vælge fremtidig leverandør. Leverandører skal herudover som regel være ISO-certificeret for overhovedet at måtte byde, hvilket indsnævrer feltet af mulige leverandører. Endelig er indkøb via udbud ofte en relativ langsommelig proces.

Ikke desto mindre er den tyske vandsektor attraktiv for leverandører af cybersikkerhed. Salg til kommunale vandforsyning- og spildevandsselskaber er gode referencer, der vidner om kvalitet og troværdighed, hvilket kan åbne døre i salgssituationer. Samtidig kan et vundet udbud hos et offentligt selskab ofte være indgangen til en række mindre men attraktive opgaver hos det pågældende selskab – vel at mærke opgaver, som ikke skal i udbud.

En række globale virksomheder udbyder cybersikkerhedsløsninger til tyske virksomheder. Der er tale om virksomheder, der har cybersikkerhed som et af flere forretningsområder. Andre vigtige aktører på markedet er mellemstore/ store specialiserede IT-virksomheder, der ofte har fokus på specifikke brancher. Puljen af leverandører, der er kvalificeret og har muskler til at løfte opgaver for offentlige virksomheder, er relativ begrænset, dvs. det er ofte de samme leverandører, der kæmper om at vinde udbud om cybersikkerhed hos de tyske vandselskaber.

Markedet for cybersikkerhed i vandsektoren i Danmark

Pt. er markedet for cybersikkerhedsløsninger i den danske vandsektor relativ lille, ligesom vækstraterne er små.

Vedtagelsen af NIS2-direktivet har (endnu) ikke affødt en stor stigning i interessen for eller efterspørgsel efter cybersikkerhedsløsninger i den danske vandsektor. Branchekendere forventer dog, at de betydelige skærpelser i NIS2-direktivet samt det seneste års øgede risiko for angreb på kritisk infrastruktur vil skubbe væsentlig til vandselskabernes forståelse, prioritering og håndtering af cybersikkerhed.

Fraværet af lovgivning og branchestandarder har betydet, at danske vandselskaber ikke har haft definitioner, rammer eller værktøjer etc. til at forstå og arbejde med cybersikkerhed.

For at kompensere herfor, har danske vandselskaber ofte henvendt sig til deres revisorer eller til konsulenthuse. Revisions- og konsulenthuse har opbygget egentlige cyberafdelinger, der har specialiseret sig i at hjælpe vandselskaber med alt fra forståelse, medarbejdertræning til strategi, ligesom de også kan hjælpe med at sammensætte tekniske løsninger via udvalgte samarbejdspartnere. Revisorerne og konsulenthusene bliver således et tryghedsskabende bindeled eller en troværdig brobygger til et område, som vandselskaberne generelt har svært ved at få greb om.

Cybersikkerhedsløsningerne, der udbydes og sælges, er i høj grad tilpasset det enkelte vandselskab. Vandselskaberne higer efter one-size løsninger eller pakkeløsninger, men en stor variation i vandselskabernes situation (f.eks. anlæg, viden og kompetencer) besværliggør dette. Størst behov har danske vandselskaber for grundlæggende awareness- og træningskurser i cybersikkerhed.

Samarbejdsområder for cybersikkerhed i vandsektoren over grænsen

Cybertruslen mod vandselskaber i Danmark og Tyskland er forøget, og vandselskaber på begge sider af grænsen har erkendt, at det er nødvendigt at forholde sig til og aktivt håndtere truslen.

I modsætning til danske vandselskaber, har tyske selskaber pga. lovgivning og branchestandarder en ramme og værktøjer til at arbejde med cybersikkerhed. Det fælles udgangspunkt har været retningsvisende for virksomhedernes arbejde og betydet både en større forståelse, accept og modenhedsniveau hos tyske vandselskaber.

På begge sider af grænsen har det hidtil dog primært været de større virksomheder i sektoren, der har implementeret processer og tiltag; mindre vandselskaber mangler ofte viden, kompetencer og ressourcer hertil.

Tyske vandselskaber er forankret i en offentlig ejerstruktur, der er kendetegnet ved forretningsgange, procedurer og kontrolprocesser. Ultimativt har tyske kommunalpolitikere ansvaret for at vandselskaberne er klædt på til at håndtere cybertruslen, og borgerne har, når de stemmer til kommunalvalg, mulighed for at udtrykke tilfredshed eller utilfredshed med dem. Ejerstrukturen og ansvarsfordelingen syntes at virke som et relativt stærkt incitament for at arbejde med cybersikkerhed.

En betydelig del af danske vandforsyningsselskaber drives ofte på frivillig basis eller af deltids- eller timeansatte, hvor der primært er fokus på den daglige drift. Danske vandforsyningsselskaber står også til ansvar for deres beslutninger og handlinger på generalforsamlinger, men de er ikke, som i Tyskland, automatisk indarbejdet i et setup med forretningsgange, procedurer og kontroller. Danske vandforsyningsselskaber har således et større råderum og friere rammer til at arbejde med cybersikkerhed.

Både danske og tyske vandselskaber er som monopolister underlagt stramme økonomiske rammer – rammer der dog vanskeliggør investeringer i nye tiltag indenfor f.eks. kvalitet, infrastruktur, klima og cybersikkerhed.

Samarbejdsområder indenfor cybersikkerhed i vandsektoren på tværs af grænsen er således bl.a.:

- Udarbejdelse og videreudvikling af branchestandarder, der matcher de nye krav i NIS2.
- Undersøgelse af mindre vandselskabers kompetence- og vidensniveau samt behov og på baggrund deraf udarbejdelse og udvikling af kompetenceforløb.
- Videns- og erfaringsudveksling om cybersikkerhed i erfagrupper med deltagelse af både vandselskaber, brancheorganisationer og leverandører af cybersikkerhed.

Referencer

Arbeitsgemeinschaft Trinkwassertalsperren e. V., Bundesverband der Energie- und Wasserwirtschaft e. V., Deutscher Bund der verbandlichen Wasserwirtschaft e. V., Deutscher Verein des Gas- und Wasserfaches e. V. – Technisch-wissenschaftlicher Verein, Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V., Verband kommunaler Unternehmen e. V. (2020). Branchenbild der deutschen Wasserwirtschaft 2020. https://issuu.com/bdew_ev/docs/2020_branchenbild-wasserwirtschaft/2

Bisgaard, Emil (2022). Hvad betyder NIS2-direktivets regler om cybersikkerhed- og informationssikkerhed for kommuner? https://kammeradvokaten.dk/nyheder-viden/nyheder/2022/06/hvad-betyder-nis2-direktivets-regler-om-cyber-og-informationssikkerhed-for-kommunerne

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2022). Sektoren und Branchen Kritis. https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html

Bundesamt für Sicherheit in der Informationstechnik (2022). Die Lage der IT-Sicherheit in Deutschland 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410

Bundesamt für Sicherheit in der Informationstechnik (2023). Gesetz zur Umsetzung der NIS-Richtlinie. https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinie/nis-richtlinie_node.html

Bundesamt für Sicherheit in der Informationstechnik (2022a). § 8a Absatz 1 BSIG - Konkretisierung der KRITIS-Anforderungen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Konkretisierung_Anforderungen_Massnahmen_KRITIS.pdf

Bundesamt für Sicherheit in der Informationstechnik (2022B). Cyber Security Strategy for Germany. https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Strategie/Cyber-Sicherheitsstrategie/cs_Strategie.html

Bundesverband der Energie- und Wasserwirtschaft e.V., Verband Kommunaler Unternehmen e.V. (2012). Leitfaden zur Wasserpreiskalkulation. Gutachten „Kalkulation von Trinwasserpreisen“. https://www.bdew.de/media/documents/Pub_20121120_Leitfaden-Wasserpreiskalkulation-klein.pdf

Center for Cybersikkerhed (2022d). Cybertruslen mod Danmark 2022. https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-danmark-2022.pdf

Dansk Standard (2023). ISO/IEC 27001 Informationssikkerhed. https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed?gclid=EAIaIQobChMIot6z4Lew_AIVtxoGAB2c1g1BEAAYBCAAEgIhlfD_BwE

DANVA (2022). Vand i tal 2022 Danmark. https://www.e-pages.dk/danva/258/

DANVA (2022b). IT- og cybersikkerhed. https://www.danva.dk/viden/it-og-cybersikkerhed/

Deloitte og Miljøministeriet (2022). Cybersikkerhed i vandsektoren. Foranalyse til cyber- og informationssikkerhedsstrategi.

Deutscher Verein des Gas- und Wasserfaches (DVGW) og Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V. (DWA) (2022). Wassersektor vor Cyberangriffen schützen – Update des IT-Sicherheitsleitfadens veröffentlicht. https://www.dvgw.de/medien/dvgw/verein/aktuelles/presse/gempi-dvgw-dwa-update-cybersicherheitsleitfaden.pdf

EnergiCert (2022). Sammen styrker vi cybersikkerheden i dansk, kritisk infrastruktur. https://energicert.dk/

EnergiCert (2022a). EnergiCERTSs trusselvurdering 6. december 2022. https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/energi/

Hansen, Regner (2022). Vandsektoren skal have en ny strategi for cybersikkerhed. https://www.danva.dk/nyheder/2022/vandsektoren-skal-have-en-strategi-for-cybersikkerhed/

Horten (2022). NIS2-direktivet: Bliv klogere på de nye regler om cybersikkerhed. https://www.horten.dk/viden/artikel2022/nis2-direktivet-bliv-klogere-paa-de-nye-regler-om-cybersikkerhed

Mikkelsen, Gert Læssøe (2002). Cybersikkerhed – standarder og rammeværker. Oplæg på konference ”Cybersikkerhed” arrangeret af JP Aurora d. 8. november 2022.

Miljøministeriet (2022). Vandsektoren – regulering og organisering. https://mst.dk/natur-vand/vand-i-hverdagen/vandsektoren/

Miljøministeriet (2022A). Hvem leverer drikkevandet? https://mst.dk/natur-vand/vand-i-hverdagen/drikkevand/hvem-leverer-drikkevandet/

Neuerer, Dietmar (2020). Cyberattacken: Großteil der Wasserversorger nur unzureichend geschützt, Handelsblatt, 26.09.2020: https://www.handelsblatt.com/politik/deutschland/sicherheit-der-wasserversorgung-cyberattacken-grossteil-der-wasserversorger-nur-unzureichend-geschuetzt/26219428.html

Konkurrence- og forbrugerstyrelsen (2019). Udviklingen i den danske vandsektors økonomi 2010-2019. https://www.kfst.dk/media/enxhlhwn/udviklingen-i-den-danske-vandsektors-oekonomiske-rammer_final.pdf

Konkurrence- og forbrugerstyrelsen (2022). Vandtilsyn. Økonomiske rammer. https://www.kfst.dk/vandtilsyn/okonomiske-rammer/

KWB, 2022. Cybersicherheit im Wassersektor. https://www.kompetenz-wasser.de/media/pages/forschung/projekte/cybersecurity/9786b9724b-1655889266/cybersicherheit-im-wassersektor.pdf

OpenKRITIS (2022). KRITIS-Sektor Wasser. https://www.openkritis.de/it-sicherheitsgesetz/sektor_wasser.html#anlagen

PWC, Michael N.C. Nielsen (2022). Ny vandsektorlov sendt i høring. https://www.ey.com/da_dk/power-utilities/ny-vandsektorlov-udsendt-i-horing

Retsinformation.dk, 2022. BEK nr 429 af 04/05/2018. https://www.retsinformation.dk/eli/lta/2018/429

Statista (2022), Höhe der Investitionen in die öffentliche Wasserversorgung in Deutschland in den Jahren 2000 bis 2020 (in Milliarden Euro).
Storgaard, Kristian (2022). Forstå lovgivning og reguleringer. Oplæg på konference ”Cybersikkerhed” arrangeret af JP Aurora d. 8. november 2022.

USD (2023). KRITIS: Die gesetzliche Grundlage. https://www.usd.de/kritis-2-die-gesetzliche-grundlage/

Verband Kommunaler Unternehmen (2022). Einigung in Brüssel zur neuen NIS 2 Richtlinie. https://www.vku.de/themen/recht/artikel/einigung-in-bruessel-zur-neuen-nis-2-richtlinie/

SDU

University of Southern Denmark

Phone: +45 6550 1000
sdu@sdu.dk
www.sdu.dk