



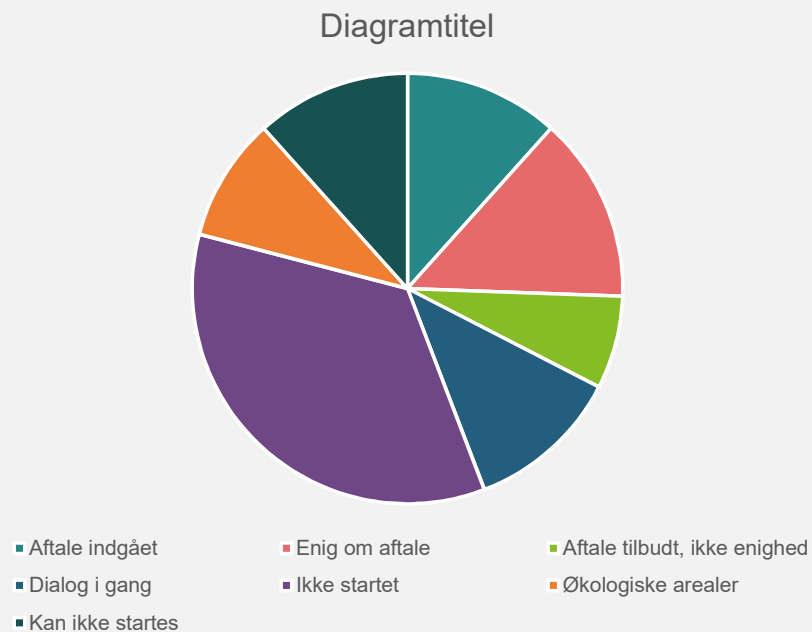
Søndersborg

Udsigt i verdensklasse

- Glokal:** Storbyen i naturen
- Grænseland:** Det bedste fra to verdener
- Handlekraft:** Vi får det til at ske

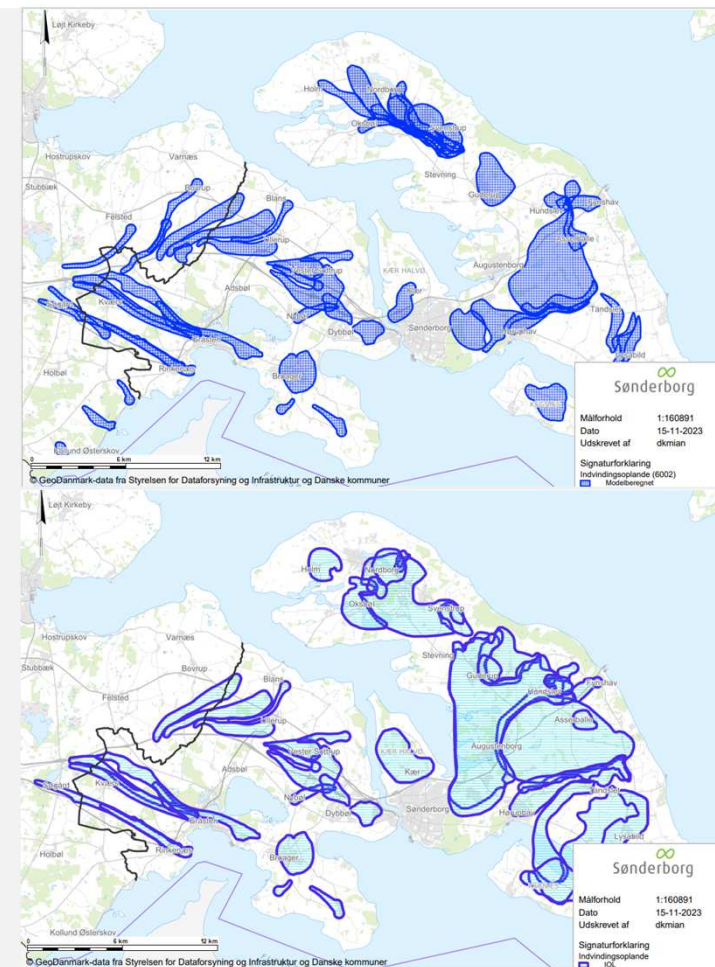
BNBO

- Totalt 43 BNBO aftaler
- Forlænget frist indtil 1 Juli 2024?
- Pligt om Påbud hvis ikke der kan indgås frivilligeaftaler



Ny model for Jylland siden

- Miljøstyrelsen har påbegyndt arbejdet på ny geologisk og hydrologisk model for Sydjylland
- Forventet færdig engang i 2024
- Genberegning af BNBO'er og indvidingsoplande tidligst 2024



Beredskabsplan

- Hvad er en beredskabsplan
- Hvad kan en beredskabsplan indeholde
 - Kontakt oplysninger på alle relevante parter (Myndigheder, entreprenører, forsikring mm)
 - Alarmeringsplan
 - Ansvarsfordeling
 - Plan for kommunikation
 - Aktionskort (brownouts, ledningsbrud, forurening, indbrud mm)
- Tilgængelig fysik og digital version

Aktionskort A – Handlingsplan ved ledningsbrud

1. Alarm indgået

- Noter tidspunkt og hvorfra alarmen kom.
- Ved telefonisk henvendelse noteres navn, telefonnummer og adresse og der spørges om omfanget og eventuelle skader.

2. Varsling

- Det ansvarlige tekniske personale underrettes jvf. Telefonliste.

3. Skadens konsekvenser

- Konsekvenserne ved nødvendig afspærring af det pågældende opland vurderes.
- Ledningsnettet fremgår af detaljerede ledningsplaner vedlagt som **bilag 15**.

4. Lokalisering og afspærring

- Bruddet lokaliseres, eventuelt ved anvendelse af lækageudstyr.
- Berørte virksomheder, institutioner og private forbrugere orienteres om afbrydelsen, hvis det er muligt.
- Eventuelt søges etableret nødvandforsyning.

5. Udbedring af skaden

- Opgravningstilladelse indhentes efterfølgende hos kommunens vejafdeling.
- Eventuelt underrettes andre ledningsejere, der kan berøres af arbejdet.
- Når skaden er udbedret vurderes omfanget af gennemskylning og desinficering.

CER direktiv (Critical Entities Resilience Directive)

- CER skal sikre kritisk infrastrukturens modstandsdygtighed mod terror, natur fare, insidertrusler og sabotage
- Identificering af Kritiske enheder
 - Identificerede kritiske enheder skal underrettes senest en måned efter identificering
- Potentielt nye krav
- Implementeres i dansk lovgivning til efteråret 2024

Fysisk beredskab(CER)

1.

Risikovurdering

- Vandværkets tilgængelighed
- Vandværkets synlige sårbarheder
- Vandværkets beliggenhed
- Vandværket som mål



Fysisk beredskab(CER)

2.

Fysisk sikring

- Perimetersikring(Hegn)
- Skalsikring(vandværksbygning, yderdøre, vinduer, borer, udvendige tanke)
- Cellesikring(indvendige rentvandstanke, filtre, administration mm)
- Adgangssikring(Hvem har nøgler til hvad?)



NIS2 direktiv

- Forventet indarbejdet i dansk lov til efteråret
- Krav om risikovurdering af OT og it-infrastruktur
- Krav om at udarbejde en it-sikkerhedspolitik
- Krav om forsyningskædesikkerhed
- Krav om uddannelse af ledelse og bestyrelse omkring it-sikkerhed
- Miljøstyrelsen analysere i øjeblikket hvilke vandværket der skal omfattes. Analysen forventes færdig i slutningen af november

Cybersikkerhed

IT sikring

- Identificering og beskyttelse af følsomme oplysninger
- Backup af data
- Opdatering af software
- Kontrol med adgangspunkter
- Sikring af OT/SRO systemer

Cybersikkerhed

- Sektionsopdeling af systemer
- Eliminering er usikker adfærd
- To-faktorgodkendelse
- Fysisk adgang

TEMA CYBERSIKKERHED TEKST: BOBBI E. JAYNE, JOURNALIST

10 gode råd om sikkerhed

DANSKVAND har bedt to it-sikkerhedspertorer med kendskab til forsyninger om at komme med tips til, hvordan vand- og spildevandselskaber bedst kan beskytte sig mod cyberkriminelle.

1 Ledelsen
Al sikkerhed begynder med ledelse. Ledelsen skal have fokus på de største sikkerhedsudfordringer og forsyningsansvar. Det indledende skridt i processen er at lave en risikovurdering, der derpå kan bruges som et prioriteringsværktøj. Dette værktøj kan være en hjælp til at vise, hvor virksomheden skal sætte ind først, og hvor virksomheden skal bruge henholdsvis flest og færrest ressourcer.

2 Segmenteret adgang
En forsyning bør generelt have et systematisk opdeling af, hvilke brugere, der har adgang til hvilke oplysninger og operationer. Brugere skal ikke kunne komme ind på det strengt nødvendige. In- og segmentering er nærmest uundgåelige på samme måde, som det er vandtætte skotter i en ubåd. Hvis der er vand- eller spildevandselskaber, som anvender samme system til administrative formål, for eksempel til at drive processer, for eksempel at tænde og slukke for pumper eller åbne og lukke for ventiler, så gælder det om at opsplitte det administrative system i så mange forskellige IT-systemer som muligt. Det ene kan bruges som springbræt til det andet. Det er en ting, hvis cyberkriminelle formår at bryde udsendelsen af regninger i nogen tid og en helt anden og langt mere alvorlig ting, hvis cyberkriminelle kan komme ind på interfaces, der regulerer drikkevandsforsyning og spildevandsstrømme.

3 Sikkerheden hos leverandører
Sikkerheden er særlig påkrævet, hvis partnere/leverandører af den ene eller anden grund har behov for adgang. Det er vigtigt at mindske angrebsflåden. En praksis om begrænset adgang kan suppleres med en kontrol af cybersikkerheden hos partnere/leverandører. Dette gælder ligeledes, hvis det er nødvendigt at lagge data i skyen. Forsyningen skal undersøge sig for, hvem der har adgang, og hvordan data transporteres. Der findes flere former for sikkerhedsattestificering. Det er næsten umuligt at undersøge det fulde, da de fleste virksomheder ikke råder over tilstrækkelige IT-ressourcer og IT-kompetencer i egen organisation.

4 Opdatering af software
Det er altafgørende at lave sikkerhedsopdateringer af software i takt med, at opdateringerne er tilgængelige. I modsat fald efterlader forsyningen en åben dør, som cyberkriminelle og andre, der måske angriber, vil være hurtige til at smutte ind på.

5 Password og tofaktorgodkendelse
Passwords er generelt et sult punkt. Mange brugeres passwords er for svage, eller brugere gæbruger et password til flere systemer. Det eneste realistiske svar er at indføre tofaktorgodkendelse. Det består i for eksempel, at skulle bruge en kode, tilsendt direkte via SMS, ud over password. Det giver et ekstra sikkerhedslag.

6 Uddannelse af medarbejdere
I it-wareness, så de undgår at blive ofre for forsøg på at narre dem. De skal afholde sig fra at klikke på links fra ukendte afsendere. En meget populær metode til at vinde er phishing. Her forsøger cyberkriminelle at få brugere eller virksomheder til at aflevere personoplysninger. Det sker ved at sende en falsk mail, der får modtageren til at tro, at kommunikation kommer fra en bank, myndighed, IT-administratør eller en person fra modtageres adressekatalog, hvortil modtageren oplyder det indtrykte område om at indsende fortrolige oplysninger pr. e-mail eller logge ind på en fiktiv hjemmeside på nettet.

7 Digital overvågning
Det kan være en god ide at indføre digital overvågning på operationel teknologisk, så det er muligt at spore eventuelle uregelmæssigheder og forsøg på påvirkning på tværs af systemet. Dette gøres med logning. Logfilene er en registrering af separat digitalt røre. En praksis med logning kan tilvejebringe svar på i realtid, og logfilerne kan desuden hjælpe til en hurtig og effektiv efterforskning af sikkerhedsændringer.

8 Beredskabsplan og venlige hackere
En beredskabsplan bør være på plads, så alle relevante medarbejdere ved, hvad de skal gøre, hvis IT-systemet er påført problemer udefra. Planen skal vise den digitale fremskridt, hvis det er nødvendigt med respons på en hændelse. Der skal desuden være en anvisning på manuelle løsninger, hvis den digitale redningsaktion går i stå. Det skal være klart, hvem der skal kontaktes. Beredskabsplanen bør tjekkes og øves af medarbejdere med faste intervaller. En beredskabsplan kan eventuelt udbygges med scenarier, hvor et hold af velkendte hackere bliver til at forsøge at finde sårbarheder i sikkerheden ved hjælp af simuleringer.

9 Fysisk adgangskontrol
En betydningsfuld cybersikkerhed involverer også en opmærksomhed om forsyningens fysiske infrastruktur. Dette er mere påkrævet i vandsektoren end i mange andre sektorer. Det er essentielt, at bygninger, anlæg og udstyr er beskyttet mod, at uvedkommende kan indhente informationer som de efterfølgende kan misbruge ved digitale angreb. Der skal lægges fokus på adgangskontrol og andre sikkerhedsprocedurer.

10 Backup
En sikkerhedskopi kan være den sidste linje, hvis IT-systemet er pålagt af uoprettelige forstyrrelser som konsekvens af et cyberangreb. Det er vigtigt at sikre sig, at denne backup er blevet testet med henblik på at kontrollere, at den faktisk er i stand til at rekonstruere systemet og reetablere det til tilfredsstillende hurtig.