

## KOMBIT bygger fælles kommunal cyberenhed

/ side 21



IT-chefer slår alarm:  
"IT-revisioner har  
taget overhånd"

/ side 10

**TEMA**  
Cyberværnet:  
Alle 98 skal med

/ side 18

DBS i Viborg:  
Fra 30 til 800 tilsyn  
på et år

/ side 34

Kommunale IT- og  
Digitaliseringsansvarlige



# Pure Storage kan nu erhverves på Staten og Kommunernes Indkøbsservice (SKI 50.03)

Pure Storage gør data management nemt med vores innovative løsninger. Med én af branchens absolut bedste brugeroplevelser, hjælper vi vores kunder med at omsætte data til værdifulde aktiver ved realisering af All-flash datacenteret kombineret med de mest moderne løsninger inden for databeskyttelse.

**Pure Storage leverer et enkelt og elegant set-up, ubesværet drift og uanede muligheder for integration samt automatiseringer.**

## Anerkendt som Leader i to af Gartner® Magic Quadrant™ rapporter

2023 Gartner® Magic Quadrant™ inden for Primary Storage.

2023 Gartner® Magic Quadrant™ inden for Distributed File Systems & Object Storage

## Energibesparende og bæredygtig IT

Reducer dit energiforbrug og gør dermed din IT mere bæredygtig; spar op til 85% i energiforbrug sammenlignet med lignende løsninger og mindsk jeres e-waste betragteligt.

## Stærk databeskyttelse, ganske enkelt

Beskyt dine data med always-on enterprise data services som kryptering, indbygget business continuity, og ransomware mitigation.

## Du går på pension - før din storage gør

Vores løsninger er intuitive, selvfornyende, bygget med innovation og bæredygtighed for øje.

Designet til lang levetid +10 år.

Hvis du vil vide mere om Pure Storage, så klik ind på [www.purestorage.com/uk/why-pure.html](https://www.purestorage.com/uk/why-pure.html) eller ræk ud til dit lokale Pure Storage Team: [nordics@purestorage.com](mailto:nordics@purestorage.com) eller [purestorage.com/uk/contact.html](https://www.purestorage.com/uk/contact.html)



# Revisionsbyrden og cyberværn ruller ind over it-afdelinger

Digitaliseringen er med til at løse opgaver lettere og smartere for ansatte i kommuner og regioner. Flere og flere rutineopgaver løses automatiseret. Om få dage sidder folk i kø digitalt for at afklare om de skal have penge tilbage i Skat eller om det er omvendt. Vi går i banken ved hjælp af MitID, får pas og kørekort i kommunen og søger om hjælp fra det offentlige til langt det meste. Vi er et af verdens mest digitaliserede samfund. Så langt så godt.

Men som en afledt effekt af digitaliseringen vælter administrative opgaver og sikkerhedsmæssige opgaver ind udefra. Vores IT-afdelinger bruger stadig mere tid på at leve op til krav fra eksterne IT-revisioner, der i dramatisk grad er taget til i omfang. Meget af det materiale revisionerne kræver, burde kunne genbruges og revisionerne burde koordineres bedre, siger en række IT-chefer, der opfordrer KL og Digitaliseringsstyrelsen til at starte en forenklingsproces af NSIS-revision. I alt er der fire større IT-revisioner. Mere kommer til fremover, som i bund og grund er en konsekvens af digital udvikling og beskyttelse af identiteter og data. Selv om det er helt klart, at der skal være orden i det kommunale hus, og at vi skal revideres efter internationale revisionsstandarder, er vi også nået til et punkt, hvor vi spørger, hvornår er nok nok? Vi slår alarm. Det er vigtigt, at reglerne ikke overimplementeres eller overgøres. Tidsforbruget i de kommunale IT-afdelinger til revision er gået over gevind. Er øget revision virkelig den bedste måde at øge sikkerheden på? Kunne nogle af ressourcerne være bedre brugt på mere operationel sikkerhed? KL mener, i lighed med KITA, "At NSIS-revisionen, der sker årligt, er unødvendig. "En årsberetning hvert andet år på NSIS burde være nok" siger KL. KL og Digitaliseringsstyrelsen siger begge, at de vil i dialog om NSIS-revisionen med henblik på at evaluere forløbet i kommunerne. Et af kritikpunkterne fra de kommunale IT-chefer går på, at opgaven om NSIS-revision varierer alt efter, hvilket revisionsfirma, der løser opgaven for kommunen.

To større revisionsfirmaer er blevet tilbudt interview i dette magasin, for at give deres version på NSIS-revision og IT-revision i al almindelighed. Men har begge takket nej.

## Cyberværnet

Et andet tema i denne udgave er cyberværnet. KL og en lang række kommuner foreslår, at alle 98 kommuner går sammen om et fælleskommunalt cyberværn, og at KOMBIT kommer ind og får en væsentlig rolle på cyber- og sikkerhedsområdet. Det bakker jeg helt op om på foreningens vegne. Dels mener jeg, det er oplagt at kommunerne samarbejder så meget som muligt på cybersikkerhedsområdet, for at få så meget sikkerhed for pengene som muligt. Dels kan jeg ikke se et bedre sted at lægge opgaven. KOMBIT har stor og god erfaring med at facilitere og levere it-ydelser til alle 98 kommuner. Det skal afklares, hvordan snitfladen mellem kommunerne, KOMBIT og andre aktører så skal være.

Og tæt på deadline har Folketinget set sig nødsaget til at udskyde lovgrundlaget for NIS2 til næste Folketingssamling, som starter i oktober 2024. Det betyder, at såvel høring som implementering bliver udskudt. Det vides ikke i skrivende stund til hvornår.



## Magasinet KITA

**Udgiver:** KITA - Foreningen af Kommunale IT- og digitaliseringsansvarlige  
Formand: Henrik Brix, Favrskov Kommune

For information om foreningen, medlemskab samt abonnement se [www.itchefer.dk](http://www.itchefer.dk)

**Redaktion:** Flemming Kjærdsdam,  
telefon 4026 3615,  
[flemming@kjaersdam.dk](mailto:flemming@kjaersdam.dk)

**Redaktionsudvalg:**  
Henrik Brix, Favrskov Kommune  
Henning Strøkjær, Guldborgsund Kommune  
Poul Venø, Herning Kommune  
Kaja Jacobsen, Egedal Kommune  
Flemming Kjærdsdam  
Louise Andersen

**Annoncer:** Louise Andersen,  
Koncept, telefon 3190 1155  
[la@koncept-net.dk](mailto:la@koncept-net.dk)

**Layout:** [www.hillerup-design.com](http://www.hillerup-design.com)

**Tryk:** Jørn Thomsen Elbo A/S



**2024**

# Husk at sætte kryds i kalenderen til de kommende arrangementer i KITA

21. og 22. marts 2024 på Hotel Koldingfjord.

## KITA Generalforsamling og Temadag 2024

Tema: Cybersikkerhed og NIS2.

Se program og tilmeld dig på [www.itchefer.dk](http://www.itchefer.dk)

2. maj 2024

## Regionsmøde - Sjælland

7. maj 2024

## Regionsmøde - Hovedstaden

22. maj 2024

## Regionsmøde - Syddanmark

22. maj 2024

## Regionsmøde - Midt/Nord

22. august 2024

## Temamøde - Region Sjælland

12. og 13. september 2024 på Hotel Koldingfjord.

## KITA Efterårsseminar 2024

Nærmere information følger.

25. september 2024

## Digitaliseringsmessen24

6. november 2024

## Regionsmøde - Hovedstaden

14. november 2024

## Regionsmøde - Syddanmark

18. november 2024

## Regionsmøde - Midt/Nord

29. november 2024

## Regionsmøde - Sjælland

**Vi glæder os til at se dig**



>>> [itchefer.dk](http://itchefer.dk)

# Indhold

MAGASINET KITA | Februar 2024

LÆS  
OM

|                                                                                            |    |
|--------------------------------------------------------------------------------------------|----|
| IT-Chef Mikael Kronstrøm, Langeland:<br>"Den sydlige halvdel af Langeland lades i stikken" | 6  |
| IT-chefer slår alarm:<br>"IT-revisioner har taget overhånd"                                | 10 |
| IT-revisioner koster kommunerne dyrt                                                       | 14 |
| IT-afdelingen i Kolding Kommune<br>har brugt næsten 5000 timer på NSIS                     | 16 |



## TEMA / CYBERVÆRNET 18-29

|                                                                                                                     |    |
|---------------------------------------------------------------------------------------------------------------------|----|
| Cyberværnet: Alle 98 skal med                                                                                       | 18 |
| Alle 98 kommuner skal stå<br>sammen om et fælles cyberværn                                                          | 20 |
| KOMBIT bygger fælleskommunal cyberenhed                                                                             | 21 |
| PwC Cyberkriminalitet:<br>"Kunstig Intelligens fylder mere i<br>cyberkriminalitet og -forsvar"                      | 24 |
| Kalundborg Forsyning efter hackerangreb i 2021:<br>"Det er kun et spørgsmål om tid, hvornår vi bliver<br>ramt igen" | 26 |
| Næstved Kommune:<br>"Cybersikkerheden er blevet en<br>stor del af dagligdagen i kommunerne"                         | 28 |



|                                                                   |    |
|-------------------------------------------------------------------|----|
| SKI 02.22<br>grøn IT datacenteraftale gennem<br>nyt indkøbssystem | 30 |
|-------------------------------------------------------------------|----|



|                                                              |    |
|--------------------------------------------------------------|----|
| Kommunerne får nyt greb om<br>gravetilladelser i landområder | 32 |
|--------------------------------------------------------------|----|

|                                                          |    |
|----------------------------------------------------------|----|
| NIS2 udsat                                               | 33 |
| KL reagerer på Datatilsynets<br>afgørelse om Chromebooks | 33 |
| DBS i Viborg:<br>Fra 30 til 800 tilsyn på et år          | 34 |





# IT-Chef Mikael Kronstrøm, Langeland: "Den sydlige halvdel af Langeland lades i stikken"

**"Jeg har ikke hørt eller set konkrete planer om opsætning af mobilmaster eller nedgravning af fiber syd for Rudkøbing," siger IT-chef Mikael Kronstrøm, Langelands Kommune. Han mener, den sydlige del af Langeland lades i stikken digitalt set.**

Efter Magasinet KITA's omtale af Langelands internetproblemer, har markedet reageret positivt, ifølge direktør Jakob Willer, Teleindustrien. TDC varslede, at de vil lukke ned for kobbernettet i hele landet inden 2030. Der er 6.000 ejendomme på Langeland, der idag får deres internetforbindelse gennem kobberkabler.

Da 80 pct. af langelænderne får internetforbindelse gennem kobbernettet, vil det i praksis betyde, at Langeland vil blive lukket ude af det digitale samfund. Siden nyheden om kobbernettets nedlukning kom frem for tre måneder siden, har TDC Net meldt ud, at de vil etablere 3.000 fibernet forbindelser på Langeland i takt med, at de lukker ned for internet gennem kobberkabler. Teleselskabet 3 er gået sammen i et partnerskab med det lokale energiselskab Ø/strøm om at ville levere trådløst internet ved at opsætte mobilmaster til 5G dækning. Ifølge 3 er der foreløbigt opstillet 11 master på Langeland. Det er det Jakob Willer Teleindustrien mener med, at markedet reagerer positivt.

## Godt med opmærksomhed fra markedet

IT-chef Mikael Kronstrøm, Langelands Kommune glæder sig over opmærksomheden fra telebranchens side.

"Der er 6.000 ejendomme på Langeland, der idag får deres internetforbindelse gennem kobberkabler fra TDC. Derfor er TDC's udmelding om at etablere 3.000 fibernetforbindelser et skridt i den rigtige retning. Men det er vigtigt at sige, at TDC er ikke forpligtet til at levere et alternativ til de 6.000 ejendomme, der mister deres internetforbindelse inden 2030. Så jeg spørger – hvad med den halvdel, der ikke får fiberforbindelse som erstatning for den lukkede kobberforbindelse? Hvad kan de gøre?" spørger Mikael Kronstrøm.

Når Mikael Kronstrøm siger, at TDC ikke er forpligtet til at levere et alternativ til de nedlukkede internetforbindelser gennem kobberkabler, skyldes det, at et bredt flertal i Folketinget ophævede TDC's forsyningspligt i 2017. Det vil sige, at hvis der markeds-mæssigt ikke er belæg for at levere en ny tidssvarende internetforbindelse som erstatning for den gamle, kan teleselskabet undlade at gøre det.

# Kan I nå at reagere på alarmerne fra jeres sikkerhedsprodukter?

**Vi hører ofte, at alarmer ikke bliver håndteret på grund af manglende tid og for mange andre opgaver**

**Lad Conscias dansktalende sikkerhedsanalytikere tage ansvaret for jeres sikkerhedsalarmer 24/7**

## Dansktalende 24/7 overvågning

Conscia tilbyder 24/7 sikkerhedsovervågning baseret på SIEM-systemer og sikkerhedsløsninger fra de største leverandører. Servicen leveres allerede til flere kommuner.

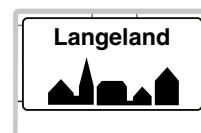
Hvis der er yderligere behov for at samle logs op fra de øvrige driftssystemer, kan Conscia hjælpe med opsætning af jeres egen SIEM-platform.

### Det får du:

- Conscia drifter platformen
- Hjælp til at oprette dashboards og sikre at logkilderne håndteres korrekt
- Dansktalende analytikere
- Tid til overs og ro i maven

Læs mere på [conscia.dk/services/managed-services](https://conscia.dk/services/managed-services) her:





Som nævnt er teleselskabet 3 gået sammen med et lokalt energiselskab Ø/strøm om at ville levere mobilt eller trådløst internet.

Mikael Kronstrøm: "Når jeg kigger på dækningen på det mobile område, og på alle de steder, hvor der er planer om at opsætte mobilmaster, så bliver de placeret i Rudkøbing området og nordpå. Det vil sige, at det største geografiske område på Langeland, - den sydlige del af øen - som også er det tyndest befolkede område, de lades i stikken. Der er jo byer sydpå, som Humble og Bagenkop, der er forholdsvis store byer, når det gøres op i Langelænder mål. Jamen ellers, er der ingen planer om udbygning af nettet – hverken med kabel eller trådløst," siger Mikael Kronstrøm.

"Eller lad mig sige det sådan. Jeg har ikke hørt eller set konkrete planer om opsætning af master og nedgravning af fiber syd for Rudkøbing," siger han.

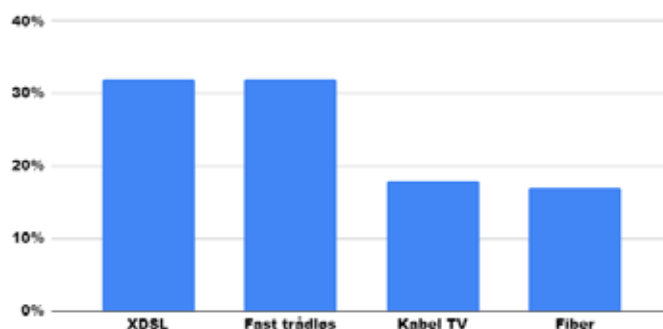
Ifølge Fyns Amts Avis kæmper Danmarks Naturfond så meget med både telefon- og internetdækningen på Skovsgaard Gods tæt på Humble, at direktøren i fonden frygter, at de kan blive nødt til at finde et nyt sted at have kontor. Når mobilen ringer forlader de kontoret og går ud til en flags-tang midt ude i haven. Det er her er den bedste mobildækning findes. Når kobberforbindelsen lukkes ned af TDC vil der ikke længere være kablet internet.

Skovsgaard Gods ligger i Humble Sogn på Sydlangeland og er en naturattraktion for børnefamilier.



**Et af de områder, som i den grad er ramt af dårlig dækning, er Langeland med en dækningsgrad helt nede på 74 pct. viser en ny statusrapport fra Byregion Fyn.**

### Langeland/ Teknologisk set:



Kobbernet er stadig den mest udbredte internetforbindelse på Langeland i 2023. Fiber er stadig den mindst udbredte internetforbindelse på Langeland i 2023.

Kilde: Byregion Fyn Digital Infrastruktur 2023



**Den sydlige del af Langeland lades i stikken digitalt set.**

IT-chef Mikael Kronstrøm, Langelands Kommune

# Infrastrukturen i tal

Infrastrukturen i tal gør det muligt for kommunerne at arbejde målrettet med at realisere merværdien af den fælleskommunale infrastruktur baseret på data og indsigter.

Læs mere på [Digitaliseringskataloget.dk](https://digitaliseringskataloget.dk)



**KOMBIT**



## IT-chefer slår alarm:

# “IT-revisioner har taget overhånd”

**Kommunernes IT-afdelinger bruger stadig mere tid på eksterne IT-revisioner, der i dramatisk grad er taget til i omfang. Men meget af det materiale revisionerne kræver, burde kunne genbruges og revisionerne burde kunne koordineres bedre, siger IT-cheferne, der opfordrer KL og Digitaliseringsstyrelsen til at starte en forenklingsproces.**

IT-revisioner er igennem de sidste fem år vokset i omfang til et niveau, der nu får IT-cheferne i kommunerne til at slå alarm. Det går ikke i længden, at IT-afdelingerne skal bruge stadig mere tid på eksterne IT-revisioner. En stor del af datamaterialet går nemlig igen fra revision til revision – det burde kunne genbruges – og tidsmæssigt burde revisionerne kunne koordineres, så ressource-trækket på IT-afdelingerne formindskes dramatisk. Magasinet KITA har talt med en række IT-chefer i kommunerne, der på

forskellig vis kan fortælle om, hvordan revisionsbyrden vokser og trækker tænder ud. Ikke bare i IT-afdelingerne, men i de stadig flere afdelinger rundt om i kommunerne, der skal involveres.

Alle IT-cheferne kan godt se rationalet bag revisionerne. De er nødvendige. Men de mener kontrollen har taget overhånd. Samtidig er der betydelig forskel på, hvor nidkært revisionerne bliver foretaget alt efter, hvilket revisionsfirma kommunerne har engageret til opgaven. Således

” **Materialekravene til de forskellige revisioner er vokset dramatisk over de sidste fem år. I 2018 var der nul livepræsentationer. I 2022 var der 22 livepræsentationer.**

IT-chef Kaj Erik Olsen, Vejen Kommune



konstaterer de, at der er stor forskel på, hvordan BDO og PwC forvalter revisionerne. Og her peger de på, at revisionsfirmaerne som private aktører selvsagt har en interesse at udvikle forretningsområdet.

I alt er der fire IT-relaterede revisioner, som kommunerne gennemgår eller inden længe skal igennem.

- Økonomisk IT-revision, hvor kommunerne skal sikre, at de digitale processer og arbejdsgangen lever op til den fornødne sikkerhed.
- MitID til borgerne (RA. Red) – en arbejdsgangsbeskrivelse, hvor det kontrolleres at kommunerne opfylder de krav, som er indgået i forbindelse med aftaler med Nets. Kommunen skal dokumentere, at det, der står i arbejdsgangsbeskrivelsen, bliver udført i praksis.
- MitID Erhverv/NSIS (National Standard for Identiteters Sikringsniveauer). Da kommuner bliver opfattet på lige fod med store erhvervsvirksomheder, kan kommuner som arbejdsgiver selv udstede medarbejdersignaturer – MitID Erhverv efter NSIS-standarder.
- NIS2 – skærpet cybersikkerhed (Network and Information Security version 2) – er ikke implementeret endnu. Men revisorer og konsulenter udbyder allerede kurser, så kommuner kan nå at blive klar til når NIS2 træder i kraft. NIS2 handler om ledelses- og bestyrelsesansvar inden for ”livsvigtige” funktioner – som energi, vand og sygehuse og opsamling af skrald.

### De stoler ikke på os

Henning Strøkjær, IT-chef i Guldborgsund kommune, der får sine IT-revisioner udført af BDO, oplever, at man ikke genbruger materialerne for de forskellige IT-revisioner. De kører som selvstændige revisioner, der ikke er koordinerede. Samtidig øges tidsforbruget i IT-afdelingen.

”Det kan godt tage over en uge – ja op til 14 dage, før vi er færdige med disse revisioner,” siger han.

Strøkjær oplever samtidig, at man i revisionerne ikke lader sig nøje med de oplysninger, som kommunernes IT-systemer giver.

”Det er ikke nok, at vi med data kan dokumentere, at medarbejderne gør det rigtigt. Nu skal revisorerne live se, at medarbejderne gør det rigtigt”.

Et eksempel er, at der skal være data og log udtræk fra medarbejdere, som har adgang til udbetaling af løn.

Her skal revisorerne simpelthen se den medarbejder, der går ind og trækker loggen direkte, så de kan kontrollere, at der ikke er fusk med den. Og den proces kan jo involvere 10-15 medarbejdere rundt om i kommunens forskellige afdelinger, som skal sidde stand by. Men er det virkelig nødvendigt?” spørger Henning Strøkjær.

### Har skiftet BDO ud med PwC

Kaj Erik Olsen, IT-chef i Vejen kommune, oplyser, at materialekravene til de forskellige revisioner er vokset dramatisk over de sidste fem år.

Han har oplevet, at revisionerne er blevet stadig mere omfattende og besværlige. Derfor har Vejen Kommunes IT-afdeling skiftet BDO ud med PwC, hvor man oplever, at arbejdsgangen er en smule mere smidig, f.eks. omkring de såkaldte penetrations-tests, hvor IT-systemernes sikkerhed afprøves. Han vurderer, at Vejen kommune alene bruger tre fuldtidsstillinger på IT-revision.

Kaj Erik Olsen pointerer, at udgangspunktet for revisioner er vejledninger fra Digitaliseringsstyrelsen, som er åbne for fortolkning.

”Men disse vejledninger skal jo ikke fortolkes som om det gjaldt IT-revisioner i f.eks. Nets, der bør være langt mere omfattende end de er i en kommune som vores,” siger han og peger ligesom Henning Strøkjær fra Guldborgsund på, at mere af det omfattende materiale, der går igen i revisionerne, må kunne genbruges. Han nævner også antallet af livepræsentationer sammen med revisor som en årsag til det stigende tidsforbrug. I revisionen i 2018 var der nul livepræsentationer. I 2022 var der 22 livepræsentationer, viser Vejen Kommunes opgørelse.

### Tidligere tog det en formiddag

Henrik Brix, IT- og digitaliseringschef i Favrskov kommune og formand for KITA, er også pikeret over den tid, der efterhånden går med at få gennemført alle IT-revisionerne.

”Nu har jeg haft 25-års jubilæum i det kommunale. Den første IT-revision foregik efter et koncept, der hed, at hver tredje år lavede man en total revision. I de to år imellem tjekkede man op på, om det, der skulle rettes, var rettet. Der gik måske en halv dag og en frokost. Nu er vi oppe i, at der til hver revision er aftalt to dage plus forberedende møder. Efterfølgende kommer der en masse opgaver til os. Med alle de revisioner, der er kommet, vil jeg tro af arbejdet er vokset med en faktor 10,” siger Henrik Brix. Også han mener, at revisionerne må kunne forenkles, materialer genbruges og arbejdet samordnes på bestemte dage. Han opfordrer KL og Digitaliseringsstyrelsen til at gå ind i en dialog, der har til formål at forenkle revisionsbyrden.

### BDO: Jamen det går godt

De fleste IT-revisioner foretages af BDO og PwC, men også Deloitte og i mindre grad EY er inde på dette forretningsområde, som er udviklet kraftigt i de senere år.

Indtrykket er generelt, at BDO fortolker opgaven meget omfattende, mens det i andre kommuner føles lidt nemmere at samarbejde med PwC.

– fortsættes på side 12 ►►

Partner i BDO, Brian Bomholdt, der er ansvarlig for BDO's IT-revisi-  
oner på det kommunale område afviser dog, at BDO er usmidige.  
"Vi genbruger materialer, hvor det er det muligt og aftaler timing  
individuelt med kunderne. Der er naturligvis læring og erfaring  
at genbruge, men vi skal også altid kunne stå på mål for vores  
arbejde i de konkrete sager," siger han.

Han tilføjer, at der er hans oplevelse, at "BDO har et godt samar-  
bejde med kommunerne".

"Det er vores opgave at foretage en ekstern og uafhængig revi-  
sion, men vi bruger naturligvis den feedback, vi får til at forbedre  
vores leverancer, her under samarbejdet med den enkelte kommu-  
ne," tilføjer han.

### Digitaliseringsstyrelsens vejledninger for brede?

Opdragsgiverne for de forskellige revisioner er i vid udstrækning  
Digitaliseringsstyrelsen, der udformer revisionsvejledninger, som  
private revisionsfirmaer fortolker og iværksætter overfor kommu-  
nerne, der hyrer dem ind til at foretage revisionerne.

Et kritikpunkt går på, at Digitaliseringsstyrelsens vejledninger til re-  
visionerne er for generelle og brede, hvilket efterlader et for stort  
spillerum for revisionsfirmaerne til at udvikle deres forretnings-til-  
bud på området.



**” Nu er vi oppe i, at der til hver revision  
er aftalt to dage plus forberedende møder.  
Efterfølgende kommer der en masse opgaver til os.  
Med alle de revisioner, der er kommet, vil jeg tro  
af arbejdet er vokset med en faktor 10.**

IT- og digitaliseringschef Favrskov Henrik Brix

**Magasinet KITA har stillet nedenstående spørgsmål til Digitaliseringsstyrelsen vedr. IT-revisionerne. Det er Christian Plaschke, Kontorchef i Kontor for MitID Erhverv og digitale serviceområdet, der svarer.**

- **De interviewede kommuner efterlyser flere præcise krav fra Digitaliseringsstyrelsen vedrørende NSIS-revision. Kan det lade sig gøre?**  
Digitaliseringsstyrelsen arbejder i øjeblikket på en evaluering og opdatering af NSIS-vejledningen, NSIS-revisionsvejledningen samt NSIS-standarden. Evalueringen finder sted med inddragelse af anvenderne, herunder bl.a. FSR – danske revisorer og Kommunernes Landsforening (KL), ligesom produkterne vil blive sendt i offentlig høring. Evalueringsforløbet forventes afsluttet medio 2024.
- **Kommunerne fremfører "uensartet implementering" fra revisorerne side, da det afhænger af, hvilket revisionsfirma kommunen har valgt?**  
NSIS-standarden er såkaldt resultatorienteret, dvs. at der skal opnås en vis grad af sandsynlighed for sikkerheden i løsningerne, men måden sikkerheden opnås kan være forskellig. Revisionsvejledning og NSIS-vejledning er udarbejdet for at give støtte til revisionsarbejdet. Det er en del af evalueringen at undersøge, om vejledningerne kan forbedres yderligere.
- **KL kommer med et ønske om årsberetninger hvert andet år. Er det muligt at sænke frekvensen af NSIS-revision?**  
Det er blandt andet noget af det, som skal undersøges i forbindelse med evalueringen.



**” Det er ikke nok, at vi med data kan dokumentere,  
at medarbejderne gør det rigtigt. Nu skal  
revisorerne live se, at medarbejderne gør det rigtigt.**

IT-chef Henning Strøkjær, Guldborgsund.

# Integration til lønsystem letter dokumentation og øger sikkerheden

*I fire år har Nyborg Kommune anvendt ID Connects løsning til styring af kommunens it-brugere. Seneste udvidelse af løsningen sikrer, at der nu er integration til Nyborg Kommunes lønsystem. Det har resulteret i fordele, der er til at få øje på.*

Nyborg Kommune stod over for en udfordring, hvor dokumentation og sikkerhed omkring brugeroprettelser og rettigheder i deres it-miljø skulle forbedres.

- Tidligere var det kompliceret at dokumentere de ændringer, vi foretog i vores Active Directory, hvilket gjorde den årlige revision besværlig og tidskrævende. Derudover måtte vi sande, at der var usikkerhed omkring vores oprettelser og nedlæggelser af brugere, hvilket kunne føre til fejl og sikkerhedsrisici, fortæller Thomas Christensen, der er it-driftskonsulent med ansvar for Nyborg Kommunes datacenter og servermiljø.

## Ny funktionalitet i ID Connect-løsningen

Nyborg Kommune udvidede deres eksisterende ID Connect-løsning, så den i dag integrerer med deres lønsystem og dermed udgør fundamentet for brugeroprettelser og -rettigheder.

- Denne løsning har gjort det muligt for os at automatisere oprettelser og nedlæggelser af brugere baseret på oplysninger direkte fra lønsystemet. Dermed har vi skåret manuelle handlinger i vores Active Directory væk, hvilket har forbedret både vores dokumentation og sikkerhedsniveau, fortæller Thomas Christensen.

Tidligere blev en bruger oprettet, når den pågældendes leder havde udfyldt og indsendt en digital blanket til it-afdelingen, som herefter kopierede brugeren i kommunens Active Directory.

- Vi måtte erkende, at det skabte usikkerheder omkring diverse data, og risikoen for fejl var mulig. Med den nye arbejdsmodel oprettes en tom bruger, som ikke er behæftet med nogen informationer, i systemet, hvor de hurtigt og enkelt kan tildeles de korrekte roller og adgange, siger Thomas Christensen.

I forhold til NSIS kan Nyborg Kommune nu også bevise, at de brugere, der skal

være oprettet, også er oprettet. Og med integrationen til lønsystemet er processen sikker.

## Fordele, der kan mærkes

Ifølge Thomas Christensen er de centrale gevinster ved den nye funktionalitet, at dokumentations- og sikkerhedskrav overholdes, men derudover er der fulgt andre fordele med ID Connects løsning.

- Inden længe kan vores afdelingsledere selv initiere og administrere brugeroprettelser direkte – og helt uafhængigt af it-afdelingen – hvilket forenkler processen og frigør tid generelt i organisationen.

- Brugeroplevelsen er også forbedret i Nyborg Kommune. Med den nye funktionalitet er det muligt at have flere ansættelser på én brugerkonto, hvilket gør det mere brugervenligt for de medarbejdere, der har flere funktioner – og dermed roller – i kommunen, forklarer Thomas Christensen

### Konkrete fordele for Nyborg kommune

- Markante forbedringer i forhold til dokumentation, sikkerhed og effektivitet i brugeradministrationen
- Automatiseringen af processerne har frigivet ressourcer, forbedret brugeroplevelsen og styrket sikkerheden
- Resultatet er en mere effektiv og pålidelig it-drift i kommunen

## Dokumentation og sikkerhedsniveau

Den nye lønintegration er en videreudvikling af den ID Connect-løsning, vi implementerede for flere år siden. Ud over at vi kan dokumentere og logge tildeling af brugernes adgang til alle vores fagsystemer, er det nu også muligt at se, hvornår brugerne er oprettet, og at de kommer fra lønsystemet, der fungerer som autoritativ kilde for disse ansættelsesforhold. Det gør det muligt for os at,

for opretholde retvisende dokumentation og et solidt sikkerhedsniveau, forklarer Henrik Dyrhøj, der er it-driftsleder i Nyborg Kommune.

## Next step er NSIS-godkendelse af vikaroprettelser

Nyborg Kommune er fortsat i gang med at implementere yderligere funktionalitet og integrationer med ID Connect-løsningen. Den endelige test af straksoprettelse af vikarer til sundheds- og plejepersonale er netop gennemført. Det betyder, at plejepersonalet nu kan få tildelt sikker og entydig adgang til KMD NEXUS. Ydermere kommer op mod 100 nye brugere til at oprette vikarer og tildele adgang uden hjælp fra it-afdelingen. Løsningen er integreret til FK-adgangsstyring og udnytter dermed den fælleskommunale infrastruktur endnu bedre.

Løsningen gør det muligt for sundhedspersonalet at være mere uafhængige af it-afdelingen – og deres åbningstider – og som en sidegevinst er det ligeledes med til at sikre, at processerne omkring vikaroprettelser nu også kan NSIS-godkendes.

### Om ID Connect

- Grundlagt i 2018
- Antal medarbejdere: 10
- ID Connect leverer en dansk-udviklet IAM Software as a Service-løsning
- Løsningen udnytter den fælles kommunale infrastruktur sammen med udgangspunkt i kommunens lokale IT-systemer herunder Microsoft Active Directory
- Fokus er brugerstyring og adgangskontrol
- Mere info på [idconnect.dk](http://idconnect.dk)



# IT-revisioner koster kommunerne dyrt

Antallet af IT-revisioner i landets kommuner er støt stigende – både i omfang og antal. Det er krav, der kommer udefra, og i takt med at digitaliseringen breder sig, bliver omfanget af hver IT-revision større. Vi har i nedenstående skitseret IT-revisionerne, som kommunerne bliver mødt med.

1

## Økonomisk revision og IT-revision

Den økonomiske revision har været gældende i mange år. Herudover kommer også IT-revisionen, som skal sikre, at de digitale processer og arbejdsgange, lever op til den fornødne sikkerhed. Her skal den eksterne, godkendte revisor kontrollere og kvalitetssikre, at kommunen opfylder internationale standarder på området. Der foretages revision af forretningsgange og interne kontroller inden for IT. Myndighed er Indenrigs- og Boligministeriet.

&lt;&lt;&lt;

2

## MitID til borgerne

En arbejdsgangsbeskrivelse af MitID til borgerne (RA red). Her skal kommunerne opfylde de krav som er indgået i forbindelse med aftale med Nets. Myndigheden er Digitaliseringsstyrelsen. Den eksterne revisor skal kontrollere, at kravene bliver opfyldt. Kommunen skal dokumentere, at det, der står i arbejdsgangsbeskrivelsen bliver udført i praksis. Dokumentation omfatter brugeradgang, hændelseslogs og diverse opfølgninger som beskrevet. Man kan godt sige, at sikkerhedsmæssigt og revisionsmæssigt inden for digitale identiteter opnår kommuner formelt en IT-sikkerhed, der minder om forholdene i et pengeinstitut. Og revisionsmæssigt sker det i følge internationale standarder. Der har ligeledes været kritik af, at der er gennemført to af hinanden uafhængige revisioner i overgangsperioden fra NemID til MitID. Både en revision af NemID og en revision af NSIS. Det er dobbelt op på tid og penge.

&lt;&lt;&lt;

3

## MitID Erhverv (NSIS)

MitID Erhverv/NSIS (National Standard for Identiteters Sikringsniveauer). Da kommuner bliver opfattet på lige fod med store erhvervsvirksomheder, kan kommuner som arbejdsgiver selv udstede medarbejdersignaturer – MitID Erhverv efter NSIS standarder. Det er nok den mest kritiserede IT-revision. Der er eksempler på kommuner, som har brugt tusindvis af timer på at blive certificeret efter de internationale standarder på området. Certificeringen følges op af en årsberetning, der underskrives af revisor og endelig godkendt af Digitaliseringsstyrelsen.

&lt;&lt;&lt;



### NIS2 – skærpet cybersikkerhed

NIS2 (Network and Information Security version 2) – er ikke implementeret endnu. Men revisorer og konsulenter og advokater udbyder allerede kurser. Der er endnu ikke udsendt et lovgrundlag, som organisationerne kan indsende hørings-svar om, men ifølge forlydender må det være overordentlig tæt på, hvis det skal kunne nå at træde i kraft i oktober. NIS2 handler om ledelses- og bestyrelsesansvar inden for "livsvigtige" funktioner – som energi, vand og sygehuse og opsamling af skrald. Der vil komme en national informations sikkerheds enhed, som skal føre kontrol med kommuner, regioner og private virksomheder inden for 13 sektorer. Det er endnu ikke afklaret, om kommuner bliver omfattet af NIS2. Men alle interessenter forventer det bliver tilfældet – og hermed er der lagt i kasketloven til endnu en årsberetning fra en ekstern revisor, der opfylder de internationale standarder. NIS2 er et EU-direktiv, der skal vedtages i Folketinget.

&lt;&lt;&lt;

Projektleder Jette Larsson, KL:

## "NSIS revision sker for tit"



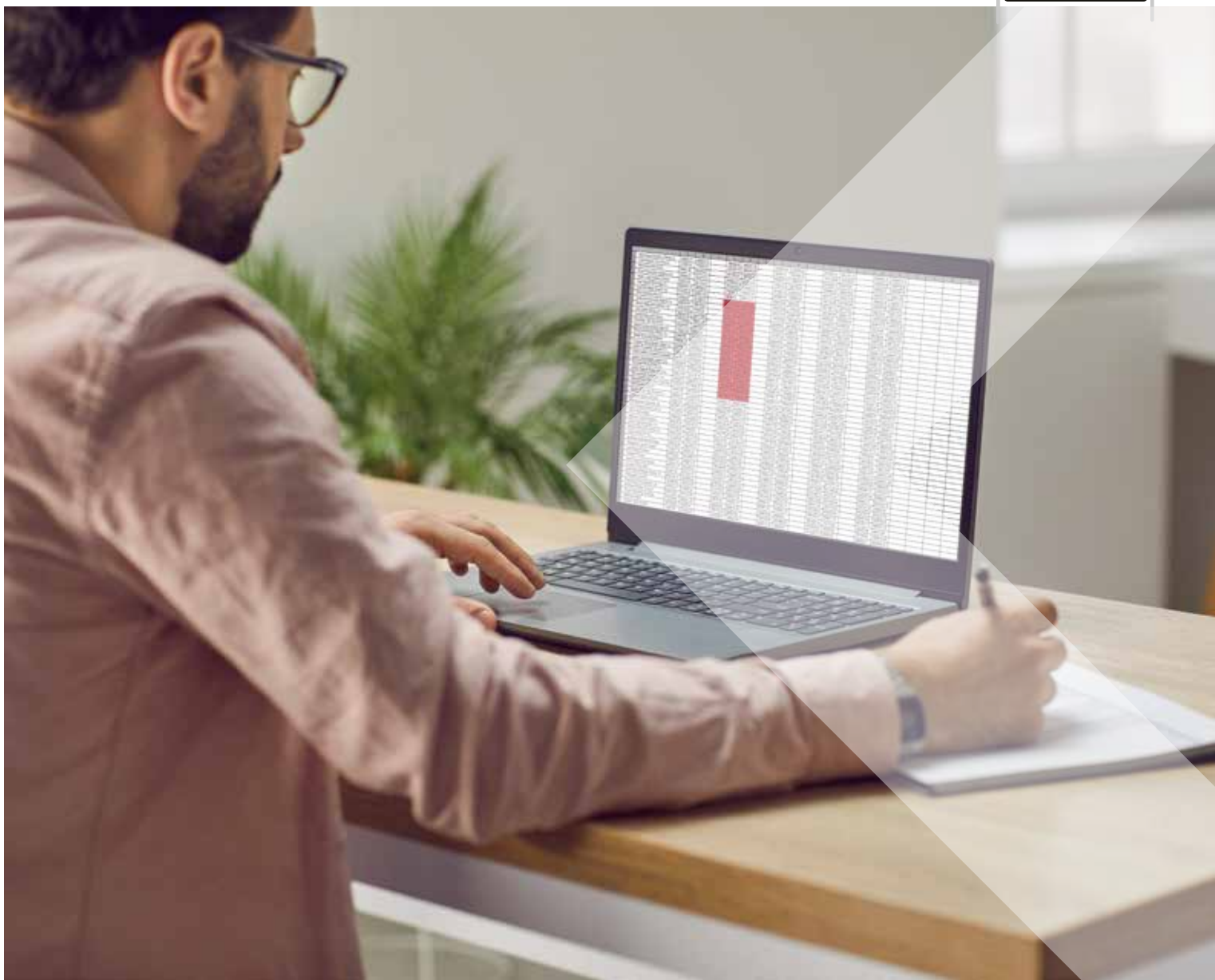
"At NSIS-revisionen sker årligt er unødvendigt efter vores opfattelse," siger projektleder Jette Larsson, KL. "En årsberetning hvert andet år på NSIS burde være nok," siger Jette Larsson.

I denne udgave af Magasinet KITA leverer IT- og digitaliseringscheferne en bredside mod den stigende IT-revisionsbyrde i landets kommuner. Den vokser både i omfang og antal – og med en kommende implementering af NIS2, har landets kommuner udsigt til endnu en årsberetning.

Jette Larssons kritik handler kun om NSIS revisionen – MitID-erhverv. "Vi har lyttet til kritikken fra kommunerne om, at revisorerne løser opgaven med NSIS forskelligt. Det er langt hen ad vejen revisorerne, der har bestemt, hvad der er gældende lov på området, fordi der ikke har været nok klarhed over, hvordan NSIS-kravene reelt skulle fortolkes. Derfor opfordrer vi til tydeligere og klarere rammer, så det ikke bliver op til den enkelte revisor at fortolke rammerne og så vi undgår, at revisorerne fortolker rammerne forskelligt," siger Jette Larsson. KL er i dialog med Digitaliseringsstyrelsen om en mere klar beskrivelse af NSIS kravene.

&lt;&lt;&lt;





# IT-afdelingen i Kolding Kommune har brugt næsten **5000 timer** på NSIS

Kolding Kommune har brugt 1,3 mio. kroner på leverandør og kodevisere og revision på NSIS/MitID Erhverv samt næsten 5000 timer internt i IT-afdelingen. Det viser en beregning som IT- og digitaliseringschef Chris B. Nørregaard, Kolding Kommune, har lavet.

Det har været en kæmpe stor opgave for de kommunale IT-afdelinger at blive NSIS/MitID Erhverv godkendt. Næsten 5000 timer i Kolding Kommunes IT-afdeling.

“Vi kunne se tingene løb stærkt undervejs i projektet. Vi havde ikke forventet, at det skulle blive så omfattende, og at vi skulle bruge så mange timer i IT-afdelingen. I takt med at vi fik os gravet ned i det og blev klogere undervejs, kunne vi godt se, vi skulle bruge meget tid på at leve op til mindstekravene. Da vi startede op med NSIS for tre år siden, har vi undervurderet opgavens størrelse,” siger Chris. B. Nørregaard.

På den anden side ønsker IT-chefen, at Digitaliseringsstyrelsen havde været mere tydelige i deres krav til kommunerne, så de forlods havde vidst, hvilken opgave de skulle løse.

Indeholdt i beløbet på 1,3 mio. kr. kommer revisorregningen fra BDO, som kommunen ikke ønsker at oplyse størrelsen på.

NSIS – National Standard for Identiteters Sikringsniveauer eller MitID Erhverv er en beskrivelse af arbejdsgange og dokumentation af medarbejdernes identiteter, der kobler sig på fællesoffentlige IT-systemer. Udgifterne og ressourceforbruget dækker i første omgang det tekniske setup og en revisorerklæring, som i sidste instans bliver godkendt af Digitaliseringsstyrelsen – og arbejdsgangene er beskrevet af Nets.

Når revisor har underskrevet erklæringen og Digitaliseringsstyrelsen har godkendt denne, er kommunens IT-sikkerhed inden for medarbejdernes digitale identiteter sammenlignelige med et pengeinstitut.

Chris B. Nørregaard: “Da Digitaliseringsstyrelsen varslede kommunerne om, at NemID Erhverv løb ud i slutningen af oktober 2023, har der været en presbold hængende over os for at komme i mål med implementeringen af MitID Erhverv og en endelig

godkendelse fra Digitaliseringsstyrelsen, som har været i drift siden november 2023.

### Anden runde

Anden runde af NSIS-certificeringen – den såkaldte type 2 – går i gang nu. Udgifter og ressourcer til den er derfor ikke opgjort, endnu.

“Vi har hidtil brugt 435.000 kroner til en ekstern konsulent for at komme i mål til tiden med den første del. Konsulenten vil vi også benytte i den anden runde. Det er en meget kompleks opgave, som meget få kan løse, og vi vil ikke selv kunne løse den eller rekruttere personale til den,” siger Chris B. Nørregaard.

Kolding Kommune har ca. 8.000 it-brugere og de 6.300 er fuldt onboardet – resten kommer på i takt med at listen over systemer, som er omfattet af MitID Erhverv, bliver udvidet.

Kolding Kommune er en stor kommune med mange medarbejdere. Derfor har kommunen valgt at løse nogle ting selv, som andre kommuner måske ikke har haft mulighed for, som udskiftningen af OCES certifikater, der bruges til MitID Erhverv. Det har ifølge IT-chefen gjort at der er blevet sparet penge til eksterne konsulenter i forberedelsesprocessen på den tekniske løsning. I stedet har de brugt flere interne timer.

I tidsforbruget er der ikke medtaget brugernes tid på opgaven.

Det er alene IT- og Digitaliserings afdelingens eget tidsforbrug.



**” Vi kunne se tingene løb stærkt undervejs i projektet. Vi havde ikke forventet, at det skulle blive så omfattende, og at vi skulle bruge så mange timer i IT-afdelingen. I takt med at vi fik os gravet ned i det og blev klogere undervejs, kunne vi godt se vi skulle bruge meget tid på at leve op til mindstekravene. Da vi startede op med NSIS for tre år siden, har vi undervurderet opgavens størrelse.**

IT- og digitaliseringschef Chris B. Nørregaard, Kolding.

# Cyberværnet: Alle 98 skal med

Alle 98 kommuner skal stå sammen om et fælles cyberværn. Derfor er KL's programleder inden for cybersikkerhed, Christian Christensen, ganske godt tilfreds med, at der er fuld opbakning fra KL's og KOMBITs bestyrelser om at gå videre med at etablere cyberværnet.

KOMBIT er lige gået i gang med at opbygge en fælleskommunal cyberenhed, som begynder at tage form. Den første aktivitet er et pilotprojekt med seks kommuner, der er med i DCIS Sund - et fælleskommunalt og regionalt cyberværn på sundhedsområdet som er drevet af Sundhedsdatastyrelsen.

Efter at Kalundborg Forsyning blev ramt af et hackerangreb i slutningen af august 2021, har virksomheden tredoblet sine investeringer i IT- og cybersikkerhed i løbet af de seneste tre år. "Det er ikke et spørgsmål om vi bliver ramt igen. Det er kun et spørgsmål om, hvornår det sker," siger forretningsdirektør Line Hoffmann, Kalundborg Forsyning.

Kalundborg Forsyning er i gang med forberedelserne til NIS2. Line Hoffmann påpeger, at lovgivningen for de nye krav om NIS2 er upræcis. "Det kan være svært at forberede sig til noget, når det ikke er helt præcist formidlet, hvad vi skal nå".

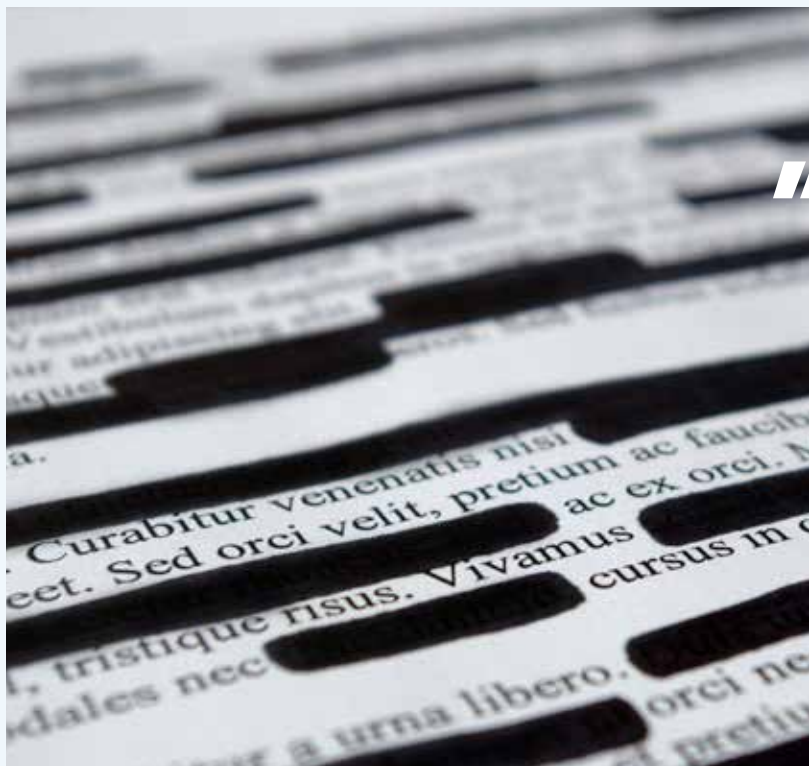
Næstved Kommune er ligeledes i gang med NIS2. "Vi ved endnu ikke, hvordan NIS2 skal implementeres og hvor meget det kommer til at fylde hos os, men vi forbereder os for ikke at komme på bagkant. Det er vigtigt at være tæt på det, der sker", siger Lars Borg.

PwC's Cybercrime Survey 2023 viser, at syv ud af 10 organisationer øger deres budget inden for cyber- og informationssikkerhed i det kommende år, hvoraf godt halvdelen vil øge budgettet med mere end 10 pct. Samtidig fortæller over halvdelen, at de er mere bekymrede for cybertruslen end for blot 12 måneder siden.

Læs artikler i  
TEMA'et om det fælles  
cyberværn

18-29

# Hvorfor bruger 17 kommuner Insight Tools?



// *Det vil vi gerne vise dig og dine medarbejdere*

*Skriv til  
info@jo-Informatik.dk  
og bestil en  
præsentation af  
værktøjet.*

Insight Tools gør aktindsigtsarbejdet meget lettere og mere sikkert:



- / Gør det lettere at beskytte borgernes data
- / Gør det nemt at søge efter følsomme oplysninger i flere dokumenter på en gang
- / Udvidet anvendelsesmuligheder ved f.eks. åbne udvalgssager
- / Fjerner følsom information permanent fra det nye dokument, som skal sendes/offentliggøres
- / Bevare originaldokumenterne med al information.
- / Sikkerhed for den rigtige modtager af aktindsigtssagen med MitID
- / Sparer tid
- / Sikrer grundighed og nøjagtighed
- / Gør scannede dokumenter og billeder søgbare og redigerbare med optisk tegngenkendelse (OCR).
- / Kan integreres med ESDH-systemet og fagsystemer





Christian Christensen,  
programleder inden for cybersikkerhed, KL

# Alle 98 kommuner skal stå sammen om et fælles cyberværn

**Alle 98 kommuner skal stå sammen om et fælles cyberværn. Ingen kommune er i sig selv store nok til at håndtere cybertruslerne individuelt. Derfor er KL's programleder inden for cybersikkerhed, Christian Christensen, ganske godt tilfreds med, at der er fuld opbakning fra KL's og KOMBITs bestyrelser om at gå videre med at etablere et cyberværn.**

KL har arbejdet intenst i snart et års tid for at få defineret en klar rolle for kommunerne i det nationale cyberforsvar. KL vil gerne gennem en politisk aftale med staten, sikre aftaler om f.eks. tekniske minimumskrav, operationelle tiltag til at opdage, reagere og forebygge cyberangreb, samt få adgang til statslige informationer om aktuelle sårbarheder og trusler. Det er endnu ikke lykkedes, men det betyder ikke, at tingene står stille.

"KL's og KOMBITs bestyrelser bakker op om det fælleskommunale cyberværn. Finansieringen er fortsat uafklaret i forhold til, hvordan vi kan få alle med. Vi har heldigvis seks kommuner med som pilotkommuner i samarbejdet med KOMBITs nye enhed. Pilotkommunerne betaler selv for opkoblingen til KOMBIT, mens KOMBIT finansierer deres egne årsværk i 2024. Og så arbejder vi videre på fuld skrue for at få finansiering til, at alle 98 kan komme med ombord i det kommunale cyberværn," siger Christian Christensen.

Kommunerne er i dag så digitalt udbyggede, at cybertruslerne udefra presser kommunerne på sikkerheden, beskyttelsen af personoplysninger og

faktisk også på muligheden for fortsat at kunne tilbyde service til borgerne. Derfor er der også rationale i, at alle 98 kommuner arbejder sammen om at beskytte den del af velfærdsstaten der er tættest på borgernes hverdag.

"Det er jo nyt, at alle 98 kommuner skal samarbejde på sikkerhedsområdet, derfor kommer vi nok til at begå fejl i starten, og kommer til at skulle lære en hel del undervejs. Det giver til gengæld kommunerne nogle nye muligheder for at få arbejdet på dette meget komplekse cyberområde. Det giver også nogle spændende muligheder i forhold til at rekruttere og fastholde specialister på cyberområdet. Der er også et nationaløkonomisk perspektiv i samarbejdet, fordi der fås mere sikkerhed for penge, end ved at skulle gøre alting selv i 98 organisationer. Det vigtigste er dog det sikkerhedsmæssige perspektiv. Muligheden for at sikre Danmark ligger i et mere forpligtende samarbejde på cyberområdet, og det ligger direkte i forlængelse af den strategi, vi lancerede for godt et år siden," siger Christian Christensen



# KOMBIT bygger fælles kommunal cyberenhed

KOMBIT er i gang med at opbygge en fælleskommunal cyberenhed, som i disse uger begynder at tage form. Den første aktivitet er et pilotprojekt med seks kommuner, der er med i DCIS Sund - et fælleskommunalt og regionalt cyberværn på sundhedsområdet som er drevet af Sundhedsdatastyrelsen.

- fortsættes på side 22 >>>

## KOMBIT bygger fælles kommunal cyberenhed

Kommunerne ser et stort behov for at gå sammen om at løse udvalgte opgaver inden for cybersikkerhed. "Cybertruslerne bliver ved med at stige, og vi har et gennedigitaliseret samfund. Det kræver en vis kapacitet og robusthed, som det ikke altid giver mening, at kommunerne opbygger hver for sig. Derfor er KOMBIT i gang med at opbygge en fælleskommunal cyberenhed," siger vicedirektør Johanne Strabo Svendsen, KOMBIT. Da KOMBIT gennemførte en Omverdensanalyse i 2023 svarede 85 pct. af kommunerne, at de ønskede, at KOMBIT skulle støtte dem i arbejdet med cybersikkerheden fremover.

"De færreste kommuner har tilstrækkelige ressourcer på området. Derfor har et stort flertal af kommunerne peget på, at KOMBIT fremover involverer sig i cybersikkerheden på vegne af kommunerne, fordi kommunerne efterlyser hjælp til det," hed det i Omverdensanalysen.

### To initiativer

KOMBIT lægger ud med to konkrete indsatser. Den første er en opdagefunktion. Den anden er et cyberforum.

Opdagefunktionen laver KOMBIT i samarbejde med Sundhedsdatastyrelsen, og de seks pilotkommuner – Favrskov, Frederikshavn, København, Næstved, Ringkøbing-Skjern og Aarhus. Det handler om at overvåge netværk og trafikken på disse netværk på sundhedsområdet. Er der afvigelse? Sker der ting, som ikke burde ske, og som der skal gribes ind over for?

Enhedschef Rasmus Vedel, KOMBIT: "Det første initiativ sker i samarbejde med Sundhedsdatastyrelsen og de seks pilotkommuner om at opbygge en





**Pilotkommunerne kommer til at teste helt konkrete ting, fordi de kommer til at køre på den platform, som Sundhedsstyrelsen har opbygget fra deres eget netværk - og Sundhedsdatastyrelsen hjælper med at kigge på tværs ved hjælp af den platform. der er opbygget hos dem.**

Enhedschef Rasmus Vedel, KOMBIT

opdagefunktion. Vi har fået lov at købe os ind på Sundhedsdatastyrelsens setup i DCIS-Sund, og derigennem kan vi opbygge en opdagefunktion i den enkelte kommune og få mulighed for at se på tværs af alle de deltagende kommuner.

“For os er det et naturligt sted at starte. DCIS Sund indeholder alle de klassiske dyder inden for cybersikkerhed. Så pilotkommunerne kommer til at teste helt konkrete ting, fordi de kommer til at køre på den platform, som Sundhedsstyrelsen har opbygget fra deres eget netværk - og Sundhedsdatastyrelsen hjælper med at kigge på tværs ved hjælp af den platform. der er opbygget hos dem,” siger Rasmus Vedel.

KOMBIT fortæller, at aftalen med de seks pilotkommuner går ud på, at kommunerne selv betaler for opkoblingen og teknologien til Sundhedsdatastyrelsens platform, og KOMBIT betaler for sit eget ressourceforbrug.

DCIS Sund har kun mandat til at se sundhedsdata på tværs af kommuner og regioner.

Rasmus Vedel: “Så, vi skal som fælles cyberenhed for kommunerne lære at skille data i sundhedssektoren fra de andre sektorer, som vi også har i kommunerne. Der er en masse ting, vi skal undersøge, som led i pilotprojektet”.

Johanne Strabo Svendsen: “Tanken med at gå ind i DCIS Sund er at komme i gang med at få konkrete erfaringer inden for området frem for at vente på finansieringen af et fælleskommunalt cyberværn. Ved at arbejde med pilotprojekter får vi også opbygget en muskel, som kan skabe værdi i samarbejdet med kommunerne. DCIS Sund er et godt sted at starte, fordi alle kommuner skal kobles op på denne platform, som Sundhedsdatastyrelsen har opbygget. Vores mål er ikke at få et vist antal kommuner med. Vi skal have alle 98 kommuner med”.

Da kommunerne bliver en del af DCIS Sund fremover, vil kommunerne kunne købe ind på den aftale, som Sundhedsdatastyrelsen allerede har.

Rasmus Vedel: “Kommunerne laver allerede rigtig meget cybersikkerhed i større eller mindre skala, og der er nogle kommuner, der er virkelig dygtige til at have styr på deres datasikkerhed.”

“Så KOMBITs enhed kommer ikke ud og siger til kommunerne, nu skal I bare høre. Det er ikke på det niveau. Det er et spørgs-

mål om at opbygge en større grad af samarbejde og konsolidere på nogle af de områder, hvor det giver mening at konsolidere.

24/7 overvågning, analyse af netværkstrafik, operativt samarbejde, projektkoordinering og implementeringsstøtte. Alle områder er relevante for alle kommuner, og det kan vi med fordel bygge op sammen,” siger Rasmus Vedel.

### Cyberforum

Parallelt med opdagefunktionen vil KOMBIT opbygge et cyberforum. Det bliver et teknisk forum, der bygger på tillid, hvor man godt “tør lufte sit beskidte undertøj”, så man hjælper hinanden ved at dele hinandens gode eller dårlige erfaringer. Forummet er et initiativ, der kommer for at blive. Det er sandsynligt, at der vil komme opgaver inden for flere områder, når opdagefunktionen har fundet noget relevant eller vi får input fra de kilder, som er tæt på cyberenheden, bl.a. Center for Cybersikkerhed og Sundhedsdatastyrelsen.

Udover varsling vil også compliance og videndeling komme med i cyberforum.

“Hvis fire kommuner er udsat for afvigelse eller et angreb, er der stor sandsynlighed for, at de resterende 94 også på et eller andet tidspunkt bliver udsat for disse hændelser. Så varsler vi, og så kan de øvrige kommuner begynde at lukke de huller, der er fundet,” siger Rasmus Vedel.

KOMBIT vurderer, at det vil tage et par år at få opbygget den fælles cyberenhed og at få alle kommuner med. Finansieringen er fortsat uafklaret, og hvis der er kommuner, som allerede har investeret i tekniske løsninger på cyberområdet, som det vil kunne tage noget tid at komme ud af igen, vil det også være medvirkende til, at det tager lidt ekstra tid. Omvendt hvis finansieringen hurtigt falder i hak, vil det kunne ske hurtigere.



**Cybertruslerne bliver ved med at stige, og vi har et gennemdigitaliseret samfund. Det kræver en vis kapacitet og robusthed, som det ikke altid giver mening, at kommunerne opbygger hver for sig. Derfor er KOMBIT i gang med at opbygge en fælleskommunal cyberenhed.**

Vicedirektør Johanne Strabo Svendsen, KOMBIT.



# **PwC Cyberkriminalitet:** **“Kunstig Intelligens fylder mere i cyberkriminalitet og -forsvar”**

Hver fjerde virksomhed siger, at de bruger AI i arbejdet med cyber- og informationssikkerhed. Yderligere hver tredje har planer om at anvende AI i fremtiden, så samlet set har mere end hveranden organisation taget AI til sig eller er ved at gøre det. Det konkluderer PwC's nylige undersøgelse om cyber- og informationssikkerhed, Cybercrime Survey 2023.

## **FAKTA**

### **Phishing er det mest brugte angreb blandt cyberkriminelle.**

Ved et phishingangreb forsøger hackere at lokke medarbejdere til at foretage en handling, der øger sandsynligheden for succes for den cyberkriminelle. Det kan være at klikke på et link til en hjemmeside eller åbne en fil, som til forveksling ligner en tjeneste, medarbejderen kender på forhånd. Når først en medarbejder interagerer med linket eller filen, kan det resultere i, at de cyberkriminelle får adgang til fortrolige oplysninger, eller at der bliver åbnet en digital bagdør ind til virksomheden.

Flere virksomheder prioriterer nu AI i arbejdet med cybersikkerhed og udviklingen inden for AI åbner nye døre i arbejdet med cyber- og informationssikkerhed, viser PwC's nye undersøgelse. Det optager især de større virksomheder og organisationer.

Partner i PwC og ekspert i cyber- og informationssikkerhed, Mads Nørgaard Madsen, siger:

"AI rummer et enormt potentiale for at transformere samfundet og måden at drive forretning på, men med potentialet følger også betydelige risici og ikke mindst etiske overvejelser, som både virksomheder og organisationer må forholde sig til. Når det gælder sikkerhedshændelser, kan AI ses som en stor trussel udefra for virksomheder og organisationer, da en AI-støttet angriber kan bruge AI til at automatisere opgaver, forbedre og sammenkøre værktøjer. Det kan føre til en højere succesrate for den cyberkriminelle".

"Men AI-værktøjer kan samtidig bruges defensivt af it-organisationer til at identificere mulige trusler gennem avancerede phishingfiltre eller til at overvåge slutbrugeres enheder for at registrere, hvis deres aktiviteter afviger fra normalen," siger Mads Nørgaard Madsen.

Så AI fylder mere både blandt de cyberkriminelle og de virksomheder, der skal beskytte sig mod de kriminelle.

### Phishingangreb topper listen

Netop phishingangreb topper listen over de hyppigste hændelser. Ifølge Cybercrime Surveyet har mere end hver anden større virksomhed således været ramt af mindst en sikkerhedshændelse, der har påvirket virksomheden negativt, inden for det seneste regnskabsår. Og af de virksomheder, der har været ramt, udgør phishingangreb 72 pct.

Mads Nørgaard Madsen fortæller, at hackerne ved hjælp af AI-værktøjer kan lave mails så naturtro og realistisk, at medarbejderne kan komme til at klikke forkert. "Det er jo ikke bare teksten, der er bedre. Det er også layoutet. De kan fodre en algoritme med et par mails fra Skat, og så laver AI-værktøjet et "look and feel", der minder fuldstændig om en ægte mail, og det tager ingen tid. Det vil vi desværre nok se mere af i 2024".

Defensivt handler det om, at der holdes øje med trafik på organisationers netværk og maskiner.

Det er jo tusindvis af hændelser, der foregår i computersystemerne. Det kan man ifølge PwC "ikke gøre effektivt nok med menneskekraft", så her kan virksomheder bruge AI og computerkraft til hele tiden at holde øje med, hvad der foregår. Analysere på det der foregår og så reagere på det. "AI-værktøjerne er så kloge i dag, at de kan reagere på uregelmæssige hændelser. Det giver virksomheden mulighed for at lukke ned for en medarbejders maskine, hvis noget ser forkert ud. Og så isolerer du maskinen og giver besked til dit overvågningscenter, og så kan de tage action på hændelsen," siger Mads Nørgaard Madsen

### Syv ud af 10 bruger mere på sikkerhed i 2024

PwC's Cybercrime Survey 2023 viser, at syv ud af 10 virksomheder øger deres budget inden for cyber- og informationssikkerhed i det kommende år, hvoraf godt halvdelen vil øge budgettet med mere end 10 pct. Samtidig fortæller over halvdelen, at de er mere bekymrede for cybertruslen end for blot 12 måneder siden.

Det er selvfølgelig truslerne udefra, der får virksomheder og organisationer til at bruge flere penge på cybersikkerhed.

Men Mads Nørgaard Madsen mener, at på trods af opmærksomheden og de øgede midler, er der en lang vej endnu.

"Der er ikke nogen hurtige løsninger. Men der er et større skifte på vej, hvor alle kommuner ved, at de skal prioritere it-sikkerhed, og alle er i gang med at foretage investeringer heri. Udfordringen er, at det tager flere år om at blive moden".

"Risikoen for cyberangreb forsvinder ikke. Den kan ikke stoppes. Vi skulle gerne nå dertil, at en kommune kan sige, at de ved alt om deres data, og hvis en kommune vil beskytte data, skal den vide, hvor data er. Det har mange kommuner svært ved, for der er mange data på mange forskellige systemer, så det handler om at få et overblik," siger Mads Nørgaard Madsen.

### Samarbejde giver stordriftsfordele

Cybersikkerhed er et anliggende for hele organisationen. Ifølge PwC flytter trusselsbilledet sig konstant, derfor er der ræson i at samarbejde om at beskytte sig på tværs af sektorer – kommuner, regioner og styrelser.

"Det er en kæmpe fordel at gå sammen om nogle af de her værktøjer til at beskytte sig mod trusler udefra. Der er virkelig stordriftsfordele ved at gå sammen om investeringer. Om det er 24/7 overvågning på et sygehus eller en kommunal hjemmepleje er i princippet underordnet, for det er den samme teknologi. Hvis det besluttes, at man skal kunne rykke ud til en hændelse, så er det samme beredskab, der er behov for på tværs af det offentlige. Derfor er der fordele for kommuner at kigge på sikkerhed samlet for kommunen, men også at gå sammen med regionerne og staten. Det vil være til gavn for alle parter," siger Mads Nørgaard Madsen.

<<<



**Det er en kæmpe fordel at gå sammen om nogle af de her værktøjer til at beskytte sig mod trusler udefra. Der er virkelig stordriftsfordele ved at gå sammen om investeringer. Om det er 24/7 overvågning på et sygehus eller en kommunal hjemmepleje er i princippet underordnet, for det er den samme teknologi.**

Partner Mads Nørgaard Madsen, PwC





# Kalundborg Forsyning efter hackerangreb i 2021: "Det er kun et spørgsmål om tid, hvornår vi bliver ramt igen"

Efter at Kalundborg Forsyning blev ramt af et hackerangreb i slutningen af august 2021, har virksomheden tredoblet sine investeringer i IT- og cybersikkerhed i løbet af de seneste tre år. "Det er ikke et spørgsmål om vi bliver ramt igen. Det er kun et spørgsmål om, hvornår det sker," siger forretningsdirektør Line Hoffmann, Kalundborg Forsyning.

Det var sent torsdag i slutningen af august 2021. Telefonen ringede hos forretningsdirektør Line Kromann, Kalundborg Forsyning. "Vi er blevet hacket," lød beskeden fra vagten. Men derudover havde vagten ikke flere informationer.

Line Kromann får samlet et team og i løbet af en times tid mødes de ved virksomheden. De finder ret hurtigt ud af, at systemet til vandforsyning og fjernvarme kører, men alle data er blevet låst af hackerne, så medarbejderne i teamet har ikke adgang til data, til internetforbindelser eller til telefonlister.

Hackerne har, ifølge Forsyningens IT-ansvarlige Mads Elmkvist, fundet en vej ind gennem en VPN-boks og efterladt en note om, at Forsyningen er blevet hacket og at de kræver en løsesum for at låse data op.

Line Kromann: "Vi ved ikke på daværende tidspunkt, hvor alvorligt angrebet er, og vi har ikke overblik over, om der er sket misbrug af data – altså om hackerne har taget en kopi og trukket data ud. Men under alle omstændigheder skal vi finde ind til vores data igen," siger Line Kromann.

## Back-up

Heldigvis havde hackerne ikke fået data med sig. Og heldigvis tager Kalundborg Forsyning back-up. Den seneste backup var fra kl. 22 – cirka

to en halv time før forretningsdirektøren bliver kontaktet første gang. Så backuppen er frisk.

"Man lærer utroligt meget af sådan en hændelse. Det er godt at vores anlæg bliver styret digitalt. Den nat fandt vi så ud af, at man også skal kunne styre sine anlæg manuelt. Men vi finder ud af at anlægget kører, og hackerne har ikke forsøgt at overtage styringen af vores anlæg. Så vi bruger ikke en masse tid på undersøgelser af angrebet. Vi læser den nyeste backup ind og så er vi i realiteten i drift," siger Line Kromann. På tidspunktet ved hackerangrebet på Kalundborg Forsyning, havde store danske virksomheder været udsat for angreb, som det kostede mange penge at rette op.

"Det er virkelig en læring for livet, man kan tage med sig. At lave backup og at opdatere software," siger Line Kromann.

Men selvom Kalundborg Forsyning slap nådigt fra hændelsen og med et begrænset tab, var det en brat opgaven for organisationen.

Line Kromann: "Heldigvis har medarbejderne i vores organisation gjort alt det, som de er blevet bedt om. Andre steder, hvor man har været udsat for noget lignende, vil man måske sige, det var en stor forandringsproces, man skulle igennem som organisation. Forandringsprojekt, hvor man taler om, at nu skal vi have nye password med flere karakterer. Nu skal vi

**” Man lærer utroligt meget af sådan en hændelse. Det er godt at vores anlæg bliver styret digitalt. Den nat fandt vi så ud af, at man også skal kunne styre sine anlæg manuelt. Men vi finder ud af at anlægget kører, og hackerne har ikke forsøgt at overtage styringen af vores anlæg. Så vi bruger ikke en masse tid på undersøgelser af angrebet. Vi læser den nyeste backup ind og så er vi i realiteten i drift.**

Line Kromann, forretningsdirektør, Kalundborg Forsyning.



i gang med at træne beredskab. Men vi er lykkedes med at komme over det uden problemer med medarbejderne, for der er jo ikke nogen, der har lyst til at være årsagen til, at vi bliver ramt igen. Fordi alle ved jo godt, at det er medarbejderne, der udgør den største risiko,” siger Line Kromann. “Ja, vi kan jo godt se det banker på derude. Vi har tracking systemer. Det handler virkelig om at være klogere end dem, og det bliver vi så nok ikke helt, fordi det er jo ikke som i gamle dage, hvor hackerne sad nede i kælderen og fiklede med en pc. De sidder i store kontorhuse med 9 til 17 jobs. Med bonusordninger og alt muligt andet lækkert. Hackere er ikke som vi tror. De er virkelig, virkelig dygtige, så det er kun et spørgsmål om tid. Inden de får banket på nok gange til at komme ind. Så det handler om, at vi får øje på det,” siger Line Kromann. Kalundborg Forsyning fortæller, at de har fremrykket sine cyberinvesteringer på grund af hackerangrebet. Det har måske ført til, at de føler de er et godt sted.

## NIS2

Kalundborg Forsyning er i fuld gang med forberedelserne til NIS2, men klandrer lovgivningen for at være upræcis, så det er vanskeligt at forberede sig.

Mads Elmkvist: “De udfordringer vi står overfor i NIS2, er særligt omkring kortlægningen af de systemer, der er, og hvem der ejer risikoen. Hvad er det for integrationer vi har, og så er der en del omkring leverandørstyring. Vi er ligesom alle andre forsyningsvirksomheder enormt afhængige af vores leverandører. Vi kan ansætte nok så mange sikkerhedsfolk og træne vores medarbejdere nok så meget. Men dér, hvor vi er afhængige af vores leverandører, er vi nødt til at afveje risikoen”.



Der er også en risiko den anden vej, når medarbejdere i Kalundborg Forsyning logger sig ind i leverandørernes systemer. Mads Elmkvist nævner det eksempel hvis der købes arbejdstøj hos Stark, så er det Starks hjemmeside, men det er en medarbejder i Kalundborg Forsyning, der logger sig ind, og det udgør en risiko. Alt det skal man igennem for at være compliant. Line Kromann: “Det helt store problem starter med GDPR området i 2018. Det er forbundet med bøder at overtræde forordningen om persondata. Da de begyndte at tale om NIS2 fik vi at vide at ligesom GDPR er NIS2 også forbundet med bøder - bare gange to – svarende til op til otte pct. af omsætningen.”

“Vi skal jo være compliant når NIS2 træder i kraft, og det er jo ikke så sjovt at vide, at vi risikerer at blive udsat for et bødeforlæg på otte pct. af omsætningen, når det ikke er helt præcist formidlet, hvad vi skal nå. Så lige nu prøver vi at arbejde os derhen, hvor vi tror NIS2 lander. Men det er forbrugernes penge, så vi skal helst ikke gøre noget for dybt eller bredt,” siger Line Kromann.

«««

## FAKTA

**Kalundborg Forsyning forsyner husstande med drikkevand og distribuerer fjernvarme i Kalundborg by, samt renser spildevand fra hele Kalundborg Kommune. Derudover leverer de overfladevand til nogle af de store virksomheder i Kalundborg.**

**” De udfordringer vi står overfor i NIS2, er særligt omkring kortlægningen af de systemer, der er, og hvem der ejer risikoen. Hvad er det for integrationer vi har, og så er der en del omkring leverandørstyring.**

Mads Elmkvist, IT-ansvarlig, Kalundborg Forsyning.



Næstved Kommune:

# “Cybersikkerheden er blevet en stor del af dagligdagen i kommunerne”

**Næstved Kommune er en af seks pilotkommuner, der er med i projektet om etableringen af et nationalt cyberværn på sundhedsområdet i samarbejde med Sundhedsdatastyrelsen og KOMBIT. IT- og digitaliseringschef Lars Borg, Næstved Kommune, siger at cybersikkerheden er en vigtig del af IT-strategien og fylder mere og mere i kommunens dagligdag.**

Projektet med DCIS Sund – det nationale fælleskommunale cyberværn på sundhedsområdet – er endnu så nyt, at IT- og digitaliseringsambasador Allan Eriksen, Næstved Kommune, omtaler det som et projekt i sin meget spæde start. “Vi tror på, at der kommer nogle interessante dialoger, om cyberværnet på sundhedsområdet, som vi gerne bidrager til”.

IT- og digitaliseringschef Lars Borg: “Vi har brugt rigtig mange ressourcer på NSIS-revision og lige nu kigger vi ind i NIS2, som vi skal være klar med ultimo 2024. Så da vi blev præsenteret for fælles kommunalt cyberværn initiativet, var vi ikke i tvivl om, at vi gerne vil være med som pilotkommune. Det, som fælles kommunalt cyberværn vil løfte på alle kommuners vegne, er meget lig det, vi selv har kigget på hardwaremæssigt – omkring netværkssikkerhed og analyse af datatrafik”. Det tæller også med for Næstved Kommune, at regionerne er med. Derfor har vi besluttet at de vil være med og har prioriteret tid og penge til at deltage i fælles kommunalt cyberværn.

Da KL i samarbejde med PwC fremlagde rapporten om det kommunale samarbejde om et fælles cyberværn for halvandet år siden, var der bred enighed blandt de 30-40 kommuner, der deltog i evalueringen,

at det var nødvendigt at løse opgaven i fællesskab frem for at gøre det hver for sig. At det skulle være et fælles KL/KOMBIT projekt.

## Pilotprojektet

Nu har KOMBIT så startet pilotprojektet om et cyberværn ved at gå ind på sundhedsområdet med DCIS Sund.

Allan Eriksen: “Hele tanken om at etablere et fælles cyberværn blandt kommuner, som traditionelt set ikke har et 24/7 beredskab, er det eneste rigtige. Vi skal have et værn, der kan reagere på unaturlige hændelser søndag eftermiddag klokken 15. Jeg kan huske nogle af de bekymringer, der var fremme i diskussionen om PwC-rapporten. Hvordan får vi alle med og hvordan får vi skabt en tryghed for borgerens data, som ligger på kommunale IT-systemer? Præmissen er, at alle kommuner skal kunne reagere, små som store. Vores egen kommune er jo ikke bedre end det svageste led, og det svageste led kan være mange steder alt efter, hvordan kæden kører. Og det samme gør sig gældende på landsplan”.

Senior IT-administratør Ole Pedersen: “Vi har scannet vores systemer for forskellige sårbarheder udefra, og det er også det man taler ind i



**” Vi opbevarer og behandler en stor del af borgernes data, og derfor er vi også nødt til som kommune at tænke det ind i vores IT-strategi. Vi har arbejdet målrettet på at blive bedre til at beskytte borgernes data, og vi sætter ressourcer af til det, fordi det er nødvendigt. Vi har også besluttet, at vi vil være en del af en fælleskommunal løsning.**

IT- og digitaliseringschef Lars Borg, Næstved Kommune

på fælles kommunalt cyberværn. Det er så udvidet og skaleret op, hvor man henter logs og data fra forskellige systemer og sender trafikmønstre op til en samlet enhed, hvor man kigger på om der er afvigelser eller en ganske lille variant.”

Allan Eriksen: ”Hvis vi får en alarm i Næstved, som vi siger, det er blot en information. Men det kan vise sig, at hvis du sætter den ind i en kategorisering på det fælles værn, at det kan være kritisk. Når DCIS Sund eller KOMBIT/KL cyberværn ligger bag, vil de have logs for 97 andre kommuner. Det kan være den sårbarhed hos os har bredt sig til misbrug et andet sted i landet og derfor samlet set bliver kritisk. Det er jo også interessant for os at få at vide, og måske skal vi lukke ned for en computer eller en tjeneste i vores egen kommune”.

### **NSIS - NIS2**

Udover at deltage i fælles kommunalt cyberværn, er kommunen også i gang med en ny revision på NSIS den såkaldte type 2 revision og forberedelsen til NIS2, som er et cyberværn på de kritiske forsyningsområder.

Lars Borg: ”Vi opbevarer og behandler en stor del af borgernes data, og derfor er vi også nødt til som kommune at tænke det ind i vores IT-strategi. Vi har arbejdet målrettet på at blive bedre til at beskytte borgernes data, og vi sætter ressourcer af til det, fordi det er nødvendigt. Vi har også besluttet, at vi vil være en del af en fælleskommunal løsning. Vi ved endnu ikke, hvordan NIS2 skal implementeres og hvor meget det kommer til at fylde hos os, men vi forbereder os for ikke at komme på bagkant. Det er vigtigt at være tæt på det, der sker. Hvis man lader noget passere eller venter, kommer man for sent. Selv om der er besparelser i kommunerne, er vi nødt til at finde pengene til sikkerhed.”

I den første NSIS-revision gik kommunerne igennem arbejdsgange og processer og om hvordan man skulle sikre medarbejdernes identiteter og borgernes data. I den anden revision skal kommunerne dokumentere det, de har sagt de vil gøre.

Lars Borg: ”Vi har fået vores NSIS-type 2 revisionserklæring i november 2023. Og en af de ting vi gjorde i Type 2 revisionen var, at alle brugere havde skiftet password. Den 8. januar 2024 havde alle 7000 brugere i Næstved Kommune skiftet password med mindst 15 karakterer. Jeg troede, vi ville få meget kritik af dette fra brugerne. Men det er gået lige omvendt. Vi har fået ros for dette,” siger Lars Borg.





# SKI 02.22 grøn IT datacenter aftale gennem nyt indkøbssystem

**SKI's dynamiske indkøbssystem for it-drift, 02.22, bliver den første aftale med fleksible grønne krav, der øges i takt med udviklingen i markedet. Energiforbruget i datacentre estimeres i dag at udgøre to-tre pct. af verdens samlede energiforbrug, svarende til energiforbruget for hele flyindustrien. ESG-direktør Katrine Pape Huldahl, SKI: "Ofte har den grønne omstilling en pris – en meromkostning, men når vi taler om serverer og storage samt grøn it-drift, går den grønne og økonomiske bundlinje hånd i hånd".**

SKI's ESG-direktør Katrine Pape Huldahl lægger ikke skjul på, at det dynamiske indkøbssystem 02.22 IT-drift har store perspektiver for den grønne omstilling. Det gælder både for de offentlige indkøbere og de leverandører af datacenterdrift, der får ordrene. Datacentre udleder lige så meget CO2 som den samlede globale flytrafik, og udledningen fra datacentre stiger støt. I 2030 forventes datacentre i Danmark at øge energiforbruget, så det udgør op til 13 pct. af Danmarks samlede energiforbrug.

"Når vi taler grøn IT-drift, så er energibesparelser i brugsfasen og effektiv datacenterdrift både godt for pengepungen og den grønne omstilling," siger Katrine Pape Huldahl.

Når det er så vigtigt for SKI at lancere nye grønne krav på 02.22 IT-drift-aftalen skyldes det, at teknologi til datacentre udleder 80 pct. af energien i driften.

Formålet med de nye grønne krav i det dynamiske indkøbssystem for IT-drift er at sænke CO2-udledningen fra datacentre. Derfor pointerer Katrine Pape Huldahl vigtigheden af, at kravene ikke er fastlåst i fire år, som på en traditionel rammeaftale, men hvor både services og leverandørfeltet kan være dynamisk.

"Vi har over de sidste to år været i gang med at kortlægge, hvilke grønne krav og tiltag vi kan implementere på IT-drift. På samme tid er vi den første indkøbsorganisation, som lancerer de nye grønne krav på området. Vi håber, at vores offentlige søsterorganisationer i EU og i Norden følger trop. De er i alt fald positive overfor vores arbejde og enorme indsats, som vi har delt med dem. Hvis vi kan gå sammen på tværs af EU og bruge de samme metoder og krav til at fremme den grønne dagsorden igennem det offentlige indkøb af teknologi til datacentre, kan vi skubbe og modne markedet i samme retning og hurtigere, end hvis vi skulle gøre det selv. Vi har også tiltro til, at hvis vi når en bred kam af ordregivere i EU-samarbejder, så kan vi hæve den grønne barre og udvikling på området," siger Katrine Pape Huldahl.

## Syv ydelsesområder

På 02.22 IT-drift kan offentlige indkøbere købe IT-drift inden for syv ydelsesområder, der dækker alt fra en enkelt server til outsourcing af hele IT-driften. Inden for fem af de syv ydelsesområ-



**” Når vi taler grøn it-drift, så er energibesparelser i brugsfasen og effektive datacenterdrift både godt for pengepungen og den grønne omstilling.**

ESG-direktør Katrine Pape Huldahl, SKI.

der, bl.a. clouddrift og co-location, har SKI defineret en række krav, der fremmer den grønne dagsorden.

I det dynamiske indkøbssystem arbejder SKI med et ”trafiklys” – med grønne, gule og røde farver – som illustrerer forskellige grader af krav efter ambitionsniveau, som man som offentlig ordregiver kan stille, når man udarbejder et konkret indkøb i systemet. Kriterierne følger de retningslinjer og adfærdskodeks, som er vedtaget og tiltrådt af EU. Hvert halve år genbesøger SKI kravene og deres inddeling i rød, gul og grøn i dialog med markedet.

SKI arbejder også på at indarbejde muligheden for, at de offentlige kunder også kan evaluere leverandørernes tilbud i det dynamiske indkøbssystem efter, hvor grønne de er. Det vil gøre det muligt både at stille krav og give flere point til den virksomhed, der tilbyder den grønneste løsning.

Det er ikke kun i Danmark, at virksomhederne vil blive mødt af nye krav for at begrænse energiforbruget af IT-driften. SKI har et tæt samarbejde med de nordiske lande og Holland, som også kigger på, hvordan de kan bruge SKI's model på deres indkøbsaftaler.

**FAKTA**

- Basiskrav er krav, som alle virksomheder i dag kan leve op til, og som SKI derfor anbefaler, at man altid tilvælger
- Kravene i grønt lys kan langt de fleste virksomheder på markedet leve op til, så de begrænser ikke konkurrencen mærkbart, ligesom de ikke – eller stort set ikke – er fordyrende
- Kravene i gult lys er mere ambitiøse end kravene i grønt lys. Her kan færre virksomheder leve op til kravene, og kravene vil forventeligt også forhøje prisen.
- Krav i rødt lys omfatter de krav, som stort set ingen kan leve op til i dag. SKI fraråder derfor som udgangspunkt at stille disse krav, da de i højere grad skal vise leverandørerne, hvad de skal sigte efter at kunne levere på sigt.

SKI er i gang med at udvide modellen med grønne krav i trafiklys til andre dynamiske indkøbssystemer i it-paletten, herunder 02.06 Standard software og 02.19 Fagsystemer.



# Kommunerne får nyt greb om gravetilladelser i landområder

Lige før folketinget gik på juleferie fik kommunerne en håndsrækning fra Christiansborg, da en ændring i vejloven gør kommunen til myndighed om gravetilladelser i landområder med private fællesveje. Hidtil har det været den enkelte lodsejer eller grundejerforening, som skal godkende gravetilladelser på private fællesveje til fiberselskabet. Med den nye ændring i vejloven fra 1. januar 2024, bliver kommunen vejmyndighed i landzoner.



Ifølge Fiberalliancen, der repræsenterer energiselskaberne der udruller fibernet, er der årligt hundrevis af sager om nabostridigheder, der stopper fiberprojekter i landområder.

“De svære gravevilkår har været med til at forhindre, forsinke eller fordyre anlægsprocessen for fibernet i landzoner med det resultat, at et stigende antal husstande og virksomheder i landområder afskæres fra at få adgang til hurtige internetforbindelser. Vi ser hundrevis af sager om året, hvor det ikke handler om andet, end at naboer er uenige med hinanden,” siger brancheforfatter Thomas Woldiderich, Fiberalliancen.

Humlen består i, når der skal graves fiber i jorden uden for de store byer i kommunerne, ude i landzonerne, er der en masse private fællesveje, som grundejere eller grundejerforeninger ejer. De private fællesveje kan være ret lange, og neden for enden af vejen, kan der bo nogen, der gerne vil have fibernet. For at komme derned, skal der graves langs med private fællesveje og her skal fiberselskabet have tilladelse til at grave fra de grundejere, der ligger der. Og hvis de siger nej, har det spændt ben for udrulningen af fiber til dem, der ønsker det.

“Vi har som sagt i hundrevis af den slags sager om året, hvor den digitale infrastruktur bliver kørt ud på et sidespor – uden at kommunen eller fiberselskabet reelt har kunnet gøre noget. Det nye er, at nu kan kommunen som vejmyndighed i landzoneområder gå ind og skære igennem og give gravetilladelsen, hvis kommunen godkender fiberprojektet. Det har kommunerne hele tiden kunnet gøre i byzonerne, men ikke i landzonerne. Nu kan de også give gravetilladelsen på private fællesveje i landzoner. Lovændringen er godt for fiberudrulningen i landområder og dermed får vi ligestillet land og by,” siger Thomas Woldiderich.

Med de nye regler får fibernetselskaberne mulighed for at anmode kommunen om at meddele tilladelse til at placere fiberkabler på private fællesveje i landzoner i de tilfælde, hvor der ikke kan opnås enighed med lodsejeren.

# NIS2 udsat

Lovforslagene var oprindeligt planlagt til at blive fremsat for Folketinget i første kvartal af 2024, men på grund af lovarbejdets kompleksitet og omfang er det blevet nødvendigt at udskyde fremsættelsen til næste folketingssamling i oktober 2024.

Det betyder, at Danmark kommer til at overskride den implementeringsfrist, der i direktiverne er fastsat til den 17. oktober 2024.

”Det lovforberedende arbejde har taget længere tid end forventet. Det kan jeg kun beklage. Jeg ved, at virksomheder og myndigheder lægger et stort arbejde i at blive klar til at arbejde efter de nye

regler. For stadig at give erhvervsliv og myndigheder de bedste muligheder for at forberede sig på de kommende regler, arbejder Forsvarsministeriet på at sende lovforslagene i offentlig høring så hurtigt som muligt,” siger forsvarsminister Troels Lund Poulsen (V).



## KL reagerer på Datatilsynets afgørelse om Chromebooks

”Der er brug for at ændre lovgivningen, så den er tidssvarende”. Sådan lyder budskabet i et brev, som KL’s formand Martin Damm (V) netop har sendt til børne- og undervisningsminister Mattias Tesfaye (S), digitaliseringsminister Marie Bjerre (V) og justitsminister Peter Hummelgaard (S).

Brevet kommer som en reaktion på Datatilsynets afgørelse om 53 kommuners anvendelse af Google Chromebooks, Google Workspace for Education mv. I afgørelsen vurderer Datatilsynet, at der ikke er hjemmel til at videregive personoplysninger til alle de formål, der videregives i dag. Datatilsynet peger på, at det ikke kun er på skoleområdet, der er behov for en ny lovhjemmel.

”Chromebooks afgørelsen handler ikke kun om skoleområdet, men kan få konsekvenser for alle velfærdsområderne. Det er meget omfattende, og det betyder samtidig, at hele IT-landskabet vil skulle forandres. Vi har en lovgivning, som ikke er fulgt med tiden. Det spænder voldsomt ben for kommunernes arbejde. Og dét er regeringen nødt til at ændre på,” siger KL’s formand Martin Damm og fortsætter:

”Det er jo ikke et isoleret kommunalt problem. Det er en udvikling, som rammer os alle. Jeg har meget svært ved at forstå, hvorfor det er de enkelte kommuner, der skal slås med de store tech-giganter. Og det kan ikke være rigtigt, at vi skal kæmpe for at opfinde et retsgrundlag i hver enkelt sektorlovgivning. Der er brug for en fælles ramme og et fælles retsgrundlag for, hvordan vi kan bruge de digitale redskaber i den offentlige sektor. Og der er brug for det hurtigt,” siger Martin Damm.

Datatilsynet har givet et påbud til 53 kommuner om at bringe behandlingen i overensstemmelse med reglerne og anviser forskellige måder, det kan gøres på.

Kommunerne skal efterleve påbuddet fra 1. august 2024, men skal senest 1. marts tilkendegive, hvordan de har til hensigt at efterleve det.



## DBS i Viborg:

# Fra 30 til 800 tilsyn på et år

Det Fælleskommunale Databehandlersekretariat (DBS) i Viborg har skruet op for produktiviteten inden for tilsyn med kommunale it-systemer, der indeholder personoplysninger. DBS er gået fra 30 tilsyn det første år til 800 tilsyn i år to. "Det er vi helt og aldeles tilfredse med," siger sekretariatschef Henrik Houmøller Sprøgel, DBS.

Da DBS blev stiftet i begyndelsen af 2022, var det aftalt med kommunerne, at DBS skulle føre tilsyn, såfremt 20 eller flere kommuner brugte et system med en tilhørende databehandleraftale - dvs. et it-system med personoplysninger.

Sekretariatschef Henrik Houmøller Sprøgel, DBS: "Vi er kommet rigtig godt fra start. Vi har øget mængden af tilsyn fra 30 til 800 det første år. Og i 2024 udvider vi nu antallet af tilsyn, når 10 eller flere af medlemskommuner bruger et it-system med tilhørende databehandleraftale. Det vil reelt sige, vi fordobler antallet af tilsyn i forhold til det oprindelige aftalegrundlag i 2022. Det er forbundet med markante stordriftsfordele at løse opgaven i et kommunalt fællesskab".

Som nævnt var det aftalt mellem DBS og kommunerne, at der skulle føres tilsyn, hvis 20 eller flere af medlemskommuner har et givet it-system med tilhørende databehandleraftale.

"Det betød, at vi fra starten af skulle føre tilsyn med 420 it-systemer. I 2023 har DBS gennemgået mere end 1.600 it-systemer, som anvendes i kommunerne. Cirka en tredjedel af dem indeholder ikke persondata, så her skal der ikke gennemføres tilsyn. For de øvrige cirka 1.000 it-systemer fører DBS tilsyn, og en meget stor del er færdiggjort. Det har vi kunnet gøre uden, at medlemskommunerne har skullet afsætte flere ressourcer til opgaven," siger Henrik Houmøller Sprøgel.

Det er årsagen til, at DBS nu arbejder efter den nye målsætning at føre tilsyn med alle it-systemer med databehandleraftaler, der bruges af mindst 10 kommuner.

Bestyrelsesformand Erik Sørensen, DBS: "Vi har kunnet gå fra 20 kommuner til 10 kommuner – og gennemføre dobbelt så mange tilsyn af it-systemer uden at skulle bruge væsentlig flere ressourcer. Så vi kan godt sige, at vi har løst en væsentlig større opgave, end det var forudsat".

"Det positive er, vi nu har dokumentation for vores produktivitet, at vi alene inden for det første år, har vi fået så meget styr på det her og fået sat standarder for tilsyn, at kommunerne får meget mere værdi for deres penge," siger Erik Sørensen.

### Nye beføjelser

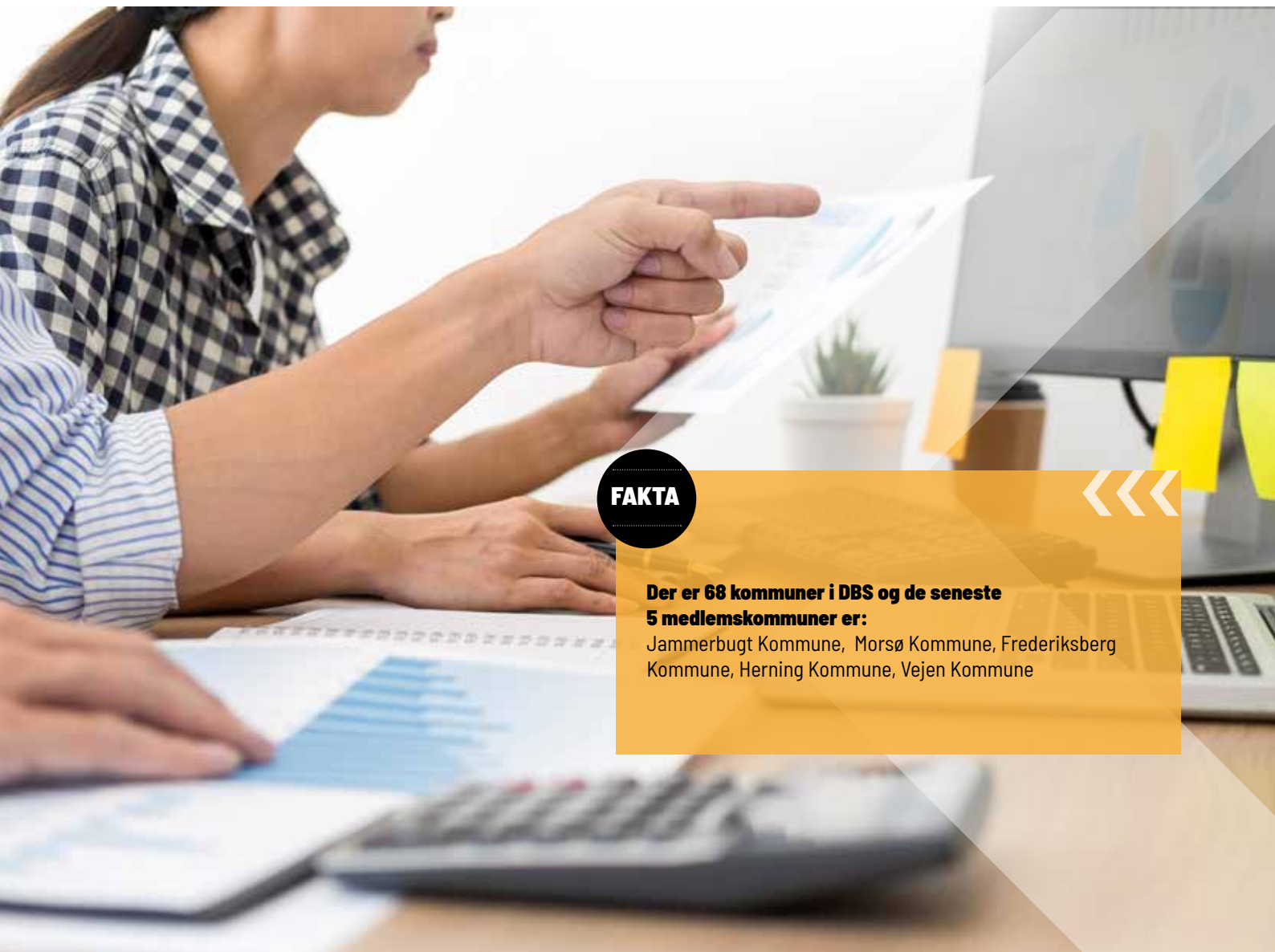
I efteråret 2023 har DBS fået udvidet sine beføjelser. Nu skal DBS ikke kun føre tilsyn med databehandleraftalerne. DBS skal også forhandle databehandleraftaler på vegne af alle kommunerne.

"Vi er så småt gået i gang med at forhandle de første databehandleraftaler med leverandørerne på plads, men DBS har på nuværende tidspunkt ikke fået landet en endelig aftale med nogen leverandører. Det er en to-delt opgave, for dels skal DBS forhandle med leverandøren på vegne af kommunerne, men det er den enkelte kommune, der skal indgå aftalen med leverandøren. Så lige nu er vi i gang med at finde ud af, hvordan kommunerne



**” Det betød, at vi fra starten af skulle føre tilsyn med 420 it-systemer. I 2023 har DBS gennemgået mere end 1.600 it-systemer, som anvendes i kommunerne. Cirka en tredjedel af dem indeholder ikke persondata, så her skal der ikke gennemføres tilsyn. For de øvrige cirka 1.000 it-systemer fører DBS tilsyn, og en meget stor del er færdiggjort. Det har vi kunnet gøre uden, at medlemskommunerne har skullet afsætte flere ressourcer til opgaven.**

Sekretariatschef Henrik Houmøller Sprøgel, Databehandlersekretariatet:



#### FAKTA

##### **Der er 68 kommuner i DBS og de seneste 5 medlemskommuner er:**

Jammerbugt Kommune, Morsø Kommune, Frederiksberg Kommune, Herning Kommune, Vejen Kommune

skal involveres i processerne,” siger Henrik Houmøller Sprøgel. Da det er den enkelte Kommune, der formelt indgår databehandlerne med leverandøren, kan DBS ikke lave en K-98 aftale, der gælder for alle, da der er store indbyrdes forskelle mellem kommunerne. DBS kan indgå et forhandlingsoplæg, som en aftale, som kan kommunen kan lave en aftale udfra.

Nu er der 68 medlemmer – opgaven bliver billigere jo flere kommuner, der melder sig ind. Frederiksberg, Jammerbugt, Morsø, Herning og Vejen er de nye kommuner, der er kommet med i DBS. Store fordele for kommuner og leverandører

DBS har som formål at sikre en ensartet praksis for tilsyn med databehandleraftaler, styrke kompetencerne på området og skabe en forbedret position for medlemskommunerne ved nye databehandleraftaler.

Erik Sørensen: ”Leverandørerne viser stor interesse for at samarbejde med os. Det er kommet i de opfølgende dialoger vi har haft med leverandørerne. Det er en klar fordel for leverandørerne at løse opgaver om databehandleraftaler i et centraliseret forum frem for at skulle gøre det enkeltvist med kommunerne. Det er nemmere at tale med et sekretariat, der repræsenterer 68 kommuner, så skal de kun tage et sted hen. Det er klart det sparer tid. Og sparet tid er som bekendt penge for alle parter”.

DBS siger at opgaven med databehandleraftaler er en kompleks opgave, som kan være svær at forstå og placere rigtigt i organisationen. Derfor giver DBS store fordele.

”DBS leverer værdiskabelse for kommunerne. Alene den produktivitetsgevinst der er skabt i det første leveår, ville ikke have kunnet realiseres, hvis kommunerne skulle løse opgaven med tilsyn og forhandling af databehandleraftaler individuelt. Det fører også til den konklusion, at DBS skaber kvalitet, da de specialister som sidder i Sekretariatet er en mangelvare, som det vil være svært for den enkelte kommune at tiltrække. Og den tredje faktor er robusthed. Hvis DBS mister en medarbejder til en privat virksomhed, så klarer vi os, Hvis det skete i en kommune, kunne det være et problem. Samarbejde med kommunerne er en grundsten i DBS. Vi kan ikke være kloge på alt. Derfor vil samarbejdet med kommunerne være helt afgørende i 2024,” siger Erik Sørensen.



# FÅ HJÆLP TIL AT STILLE GRØNNE KRAV, NÅR DU KØBER IT-DRIFT

På SKI-aftale 02.22 It-drift har vi kortlagt en række muligheder for at stille klima- og miljørelaterede krav. Disse krav er blandt andet baseret på EU's GPP-kriterier for servere og datacentre og EU's Code of Conduct inden for samme område.

Vi har omsat dem til konkrete krav, du kan stille til udbyderne af it-drift i dit indkøb, så du sænker udledningen på driften af dine it-systemer.

Dermed kan du vælge de krav, der matcher dine ambitioner, dit budget og markedet.



**Kontakt os for at høre mere om, hvordan du kan stille grønne krav når du køber it-drift.**

## Kontakt



**Jesper Ladegaard**  
Chefkonsulent  
T - 52 11 97 79  
E - jla@ski.dk



**Allan Schiellerup Bager**  
Chefkonsulent  
T - 21 27 08 27  
E - asb@ski.dk



**Ann Buer Johansen**  
Chefkonsulent  
T - 21 31 41 14  
E - abj@ski.dk



**Adam Goslett**  
Chefkonsulent  
T - 25 23 03 92  
E - add@ski.dk