MAGASINET
KITA
Kommunernes IT-Magasin

Februar 2023
ISSN 1399-7947

TEMA I / CYBERSIKKERHED
TEMA II / NSIS

Kommunale IT- og Digitaliseringsansvarlige

Talegenkendelse hjælper med at bevare høj faglig kvalitet i sagsbehandlingen

I Team Job og Udvikling i Frederikshavn Kommune indeholder den daglige sagsbehandling en del rutinepræget arbejde, og medarbejderne skal huske en masse paragraffer og nye arbejdsgange. Her hjælper talegenkendelse til at sikre et ensartet, højt fagligt niveau, og medarbejderne slipper samtidig for ondt i skulder og nakke med mindre tastearbejde.

"For mig er teknik og IT noget, der skal hjælpe os til at gøre vores hverdag nemmere, og det må man sige, at den er blevet med talegenkendelse. Især den nye version, hvor der er en utroligt høj genkendelsesgrad og flere nye funktioner, der sparer os tid. Samtidig får vi en tryghed i, at vi alle udfører arbejdsgangene med samme, professionelle niveau over for borgeren i en travl hverdag."

Sådan fortæller Erik Witt Olsen, der er Koordinerende sagsbehandler i Team Job og Udvikling i Frederikshavn Kommune og superbruger af talegenkendelse.

"Først og fremmest er værktøjet fantastisk rent ergonomisk. Flere af os døjer med dårlig skulder og ryg, og hvis jeg skulle sidde og skrive alle de her ting ind hver dag, så ville jeg være helt færdig. Hvis vi ikke havde talegenkendelse, så ville jeg få flere sygedage."

Erik Witt Olsen og hans team bruger især funktionen autotekster i deres daglige arbejde. Og teamet har endda udvidet, hvad autotekster kan bruges til.

"Ud over at bruge auto-tekster til at slippe for tastearbejde så bruger vi det faktisk også som et slags huskeværktøj. Tidligere skulle man holde styr på nye arbejdsgange eller opdaterede informationer med en mail eller en lap papir. Det fylder mentalt, fordi man ved, at der er en risiko for, at man glemmer det, eller at informationerne forsvinder," siger Erik Witt Olsen og fortsætter:

"Autotekster er den bedste opfindelse, der er. Gevinsten for mig er både tid og kvalitet. Så ved jeg, at jeg overholder kravene til indholdet i en jobsamtale og en plan. Og så er det hurtigere end at skulle huske på de forskellige ting."

Af formand Henrik Brix < **KITA**

LEDER

Hvor placerer vi ansvaret for cybersikkerheden?

Jeg lægger lige ud med at spole tiden tilbage. Bare for at få forhistorien med. I 2006 – før Kommunalreformen – var der 273 kommuner. Med Kommunalreformen blev der gennemført 66 fusioner og 32 fortsættende kommuner, så det kommunale landskab blev til 98 kommuner. Med et gennemsnitligt indbyggertal på 50.000. Favrskov, hvor jeg er IT- og digitaliseringschef, er lige præcis sådan en størrelse.

Tilbage i 2007 syntes vi, at vi var blevet store og vi havde – godt hjulpet af KMD - lagt vores kommunale it-systemer sammen med stor succes. Det var kommunalreform version 1.0.
I 2009 blev salget af KMD gennemført og KOMBIT blev etableret. Sagsbehandlingen på en række strategiske områder blev lagt ud i centre og en del til Udbetaling Danmark og ATP – under mærkatet Objektiv Sagsbehandling. I 2012 startede KOMBIT Monopolbruddet, som officielt blev afsluttet efter 10 år. Mange nye systemer har været i Fælleskommunale udbud og det er nu afsluttet. Det var Kommunalreform version 2.0.
Nu står vi ved begyndelsen til Kommunalreform 3.0 – og ligegyldigt hvor jeg kigger hen ser jeg it-sikkerhed, cybersikkerhed og cyberkriminalitet. Godt "hjulpet" af krigen i Ukraine. Går det over igen? Det har jeg vanskeligt ved at se. Dengang i version 1 i 2007 hvor vi oplevede os som store individuelle enheder, er vi nu it-mæssigt kommet tættere på en erkendelse af, at en kommune med 50.000 indbyggere blot er en brik i et stort fællesskab.
Jeg kan ikke se, hvordan vi kan løse de voksende opgaver indenfor cybersikkerhed hver for sig. Udfordringen er præcis den samme. Opgaven er stor. Det handler både om penge og kompetencer. Det giver absolut mening at samarbejde. På KITA´s seminar 2. og 3. marts på Koldingfjord får vi indlægsholdere fra Center for Cybersikkerhed, fra en moden leverandør og fra KL. Ene og alene med det formål at blive klogere på, hvordan vi sikrer et endnu bedre niveau af it-sikkerhed og beskyttelse af borgernes data ved at arbejde mere sammen.
Ikke mange kommuner har driftsovervågning 24/7/365. For mig vil det give mening at forsøge at samarbejde på så højt et niveau som muligt. F.eks. Center For Cybersikkerhed (CFCS).Men CFCS hører under forsvarsloven, så det er ikke muligt. KOMBIT er bragt i spil til at varetage udvalgte cybersikkerhedsopgaver og dermed opbygge kompetencer.
For mig er KOMBIT den bedst mulige løsning selvom kompetencerne ikke er der i dag. KOMBIT er vant – og gode – til at køre store og forpligtende K98 projekter. Vi kan også kalde det for det mindst ringe sted at placere opgaven. Kompetencerne skal jo opbygges. Jeg kan ikke se alternativet til det. Jeg ved godt der er en række kommunale samarbejder, DIGIT, DSD, IT-forsyningen, 3K m.m.. Men det batter ikke nok. For mig er det dødfødt at gøre det hver for sig eller i en række mindre fællesskaber.
I en leverandøropgørelse af IDC Nordic gennemgås 13 forskellige sektorers investeringer i it-sikkerhed. Finanssektoren bruger eksempelvis 9.511 kr. pr. medarbejder, hvilket er mere end fire gange mere end offentlig administration med 2.028 kr. pr. medarbejder.
Et cybercrime survey fra PwC viser at seks ud 10 ledere og it-fagfolk forventer markante stigninger i deres it-sikkerhedsbudgetter i 2023.
For få dage siden har CFCS hævet trusselsniveauet for cyberangreb til rød. KOMBITs nye direktør Kristian Vengsgaard, kalder det for "rød med rødt på".
Derfor lad os få en dialog om, hvor vi placerer ansvaret for cybersikkerheden og hvordan vi finder midlerne til at beskytte borgernes data i kommunerne.

KITA
Kommunale IT- og Digitaliseringsansvarlige

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**

Redaktion: Flemming Kjærsdam, telefon 4026 3615, flemming@kjaersdam.dk

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

Annoncer: Louise Andersen, Koncept, telefon 3190 1155 la@koncept-net.dk

Layout: www.hillerup-design.com

Tryk: Jørn Thomsen Elbo A/S . Oplag: 5.000

Et stærkt netværk kan booste den digitale skole

Mange skoler har et it-netværk, som ikke for alvor understøtter digital undervisning og udnytter de teknologiske muligheder. Det koster unødige ressourcer hos de it-ansvarlige og giver besvær for lærere og elever.

En digital bølge er de seneste år rullet ind over danske skoler og uddannelsesinstitutioner. Computere, smartboards, tablets og anden elektronik er i dag lige så essentielle som blyant, lineal og kridt var det før i tiden.
Digitale hjælpemidler kan skabe en mere varieret og spændende skoledag, styrke samarbejde og fællesskab og i det hele taget ruste børn og unge til et arbejdsmarked og et samfund, der er mere og mere digitalt. Men rigtig mange skoler har fortsat ikke et opdateret, sammenhængende netværkssetup, der er hele fundamentet for en velfungerende digital undervisning med eleverne i centrum.

Intelligent styring af netværk
På de fleste skoler udfordres lærernes og elevernes udfoldelser af, at teknikken driller, at enheder er svære at koble på netværket eller hopper af, når man bevæger sig rundt, og at hastigheden ikke altid er optimal. Det fører til både frustrationer og unødigt spild af elevers, læreres og it-ansvarliges sparsomme tid.

> **Den teknologiske udvikling går hurtigt, og behov og forventninger ændrer sig med kort varsel. Derfor er der rigtig mange fordele i at have en sammenhængende 'managed' løsning, som sikrer, at skolen hele tiden har et stabilt og sikkert netværk med høj ydelse. Samtidig giver det ro i maven at have fuld forudsigelighed i de løbende omkostninger og at undgå store engangsudgifter til eget udstyr," siger Karsten Høvdinghoff fra GlobalConnect.**

Samtidig er en del ikke bekendt med de mange fordele, der ligger i at kunne styre skolens netværk mere intelligent.
For eksempel tillader det rette setup at tildele forskellige roller og adgange til grupper af elever, lærere og administration, at skrue op og ned for kapaciteten og at prioritere trafikken, så elever til eksamen kan være sikre på et stabilt, trådløs netværk med høj hastighed og uden afbrydelser.

Netværk samlet ét sted
I dag kan it-ansvarlige helt slippe for at bruge deres ressourcer på planlægning, implementering og den løbende drift af skolens netværksløsning – og endda uden det slår bunden ud af budgettet.
Hvad der hidtil har krævet en række forskellige leverandører, services, hardware, interne og eksterne specialister findes nu i én sammenhængende totalløsning, som netværks- og fibervirksomheden GlobalConnect er ene om at kunne tilbyde i Danmark.
Netværksløsningen SmartConnect sikrer, at skoler har en it-infrastruktur, der altid matcher de pædagogiske behov og den teknologiske udvikling og er tilmed uden tunge økonomiske investeringer i hardware og software, som mange skoler ellers er vant til.
For et fast, lavt månedligt beløb kan skoler og uddannelsesinstitutioner via GlobalConnect få en komplet og individuelt tilpasset end-to-end netværksløsning, der er lynhurtig, stabil og fleksibel, og hvor både WAN-linjer og Wi-Fi bevæger sig gnidningsfrit gennem GlobalConnects højteknologiske fiber-infrastruktur.

Dette bør skoler overveje

- Er jeres netværk af tilstrækkelig høj standard med hensyn til kapacitet, pålidelighed og fleksibilitet?
- Giver jeres netværk mulighed for, at elever kan tilslutte deres egne enheder uden at gå på kompromis med sikkerheden?
- Er sikkerhed i jeres trådløse miljø en vigtig faktor, og har I mulighed for at bortfiltrere uønsket trafik?
- Har I behov for at kunne give forskellige roller og adgange til specifikke personer og grupper og let kunne ændre dem, fx i eksamenssituationer?
- Har I brug for kontrol med, hvilke enheder og brugere der er forbundet til jeres netværk?

GlobalConnect

Læs mere på **www.globalconnect.dk/public** eller ring på **38401600**

Indhold

MAGASINET KITA | Februar 2023

LÆS OM

TEMA I / CYBERSIKKERHED 14-30

TEMA II / NSIS 32-37

Af Flemming Kjærsdam

Bruger 6,6 milliarder på IT-sikkerhed

6,56 mia. kr. Så mange penge har danske virksomheder og offentlige myndigheder i 13 udvalgte sektorer brugt til eksterne leverandører i 2022 på IT-sikkerhed.

Cyberkriminalitet, eller truslen om samme, er blevet et stort milliardmarked i Danmark. Det fremgår af en leverandøropgørelse, som analysefirmaet IDC Nordic har udarbejdet for Magasinet KITA. Heraf fremgår, at telekommunikation, forsyningsvirksomhed og finanssektoren investerer betydeligt mere end det offentlige gør – målt i investeringer pr. medarbejder.

Associate Director Anders Elbak, IDC Nordic: "Når private virksomheder og offentlige myndigheder bruger så mange penge viser det, at IT-sikkerhed er nødvendigt og at der er en masse forskellige trusler, som de i virkeligheden er nødt til at gardere sig mod. Og så viser det også, at lederne har taget stilling til, hvad omkostningerne er ved et eventuelt sikkerhedsbrud. Ja, de er formentlig store".

Det stopper imidlertid ikke her. For mens truslerne udefra vokser, kommer der også regulatoriske tiltag fra EU med det nye direktiv NIS2.

Topscorerne

Telekommunikation, forsyningsindustri og finans investerer mange gange flere midler i IT-sikkerhed end det offentlige. Opgørelsen fra IDC omhandler alene de eksterne udgifter til leverandører.

Det er sektorer med relativt få ansatte som telekommunikation og forsyningsvirksomheder, der bruger flest penge på IT-sikkerhed. Telekommunikationsindustrien bruger årligt 23.315 kr. pr. medarbejder i eksterne udgifter til IT-sikkerhed. Tilsvarende bruger forsyningsindustrien 15.717 kr.

Finanssektoren kommer ind på tredjepladsen med 9.511 kr. pr. medarbejder. Den offentlige sektor bruger 2023 kr. pr. medarbejder på IT-sikkerhed. Så finanssektorens investeringer pr. medarbejder er i gennemsnit over fire gange større end det offentlige.

- fortsættes på side 8 »»»

NIS2 er på vej -

men er I også på rette vej, når det kommer til NIS2?

EUs nye NIS2-direktiv skal højne Europas cybersikkerhed. Direktivet stiller en række nye krav til kommuner om, hvordan de arbejder med cybersikkerhed.

Har I styr på:

- Politikker for risikoanalyse og informationssystemsikkerhed?
- Håndtering af hændelser (forebyggelse, opdagelse og reaktion på hændelser)?
- Driftskontinuitet og krisestyring?
- Kryptografi og kryptering?

BLIV KLAR TIL NIS2

Læs hvordan kommunen bliver klar til NIS2 på Conscia.dk/nis2 og download et white paper, hvor du både får overblik over direktivet, og hvad du kan gøre.

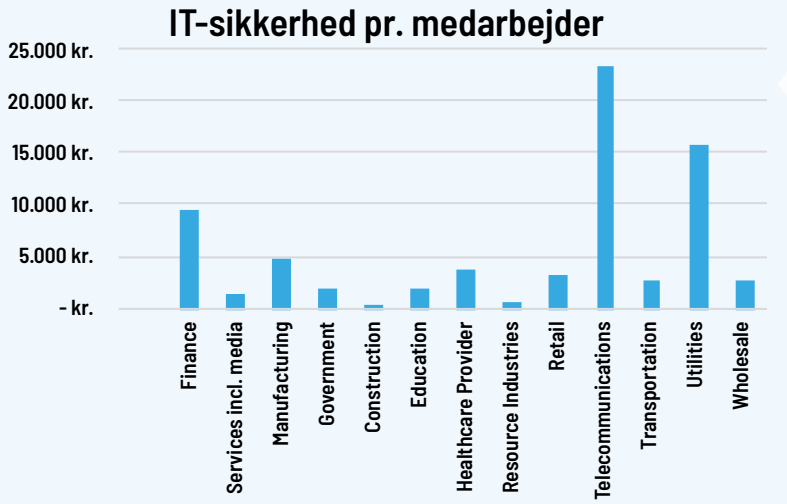
Hvem er Conscia?
Conscia er markedsledende inden for netværk, cybersikkerhed og cloud. Vi leverer sikre infrastrukturløsninger og 24/7 managed services til kunder med komplekse krav til netværk, datacenter, cloud, IOT og mobilitet.

conscia

"Dét, undersøgelsen viser, er et billede af de eksterne investeringer på tværs af sektorer. Vi ved ikke, hvor meget sektorerne bruger internt. Men det er min klare overbevisning, at finanssektoren har meget opmærksomhed internt på IT-sikkerhed. Der er en del virksomheder i den almindelige industri, der mener, at sikkerhedsbrud primært sker hos naboen. Det er ikke en holdning, man oplever i de sektorer, hvor der investeres meget. Der bliver foruden de eksterne investeringer også brugt interne ressourcer på at have fokus på sikkerheden. Der er en større modenhed i disse sektorer," siger Anders Elbak.

Når private virksomheder og offentlige myndigheder bruger så mange penge viser det, at IT-sikkerhed er nødvendigt og at der er en masse forskellige trusler, som de i virkeligheden er nødt til at gardere sig mod.

Associate Director Anders Elbak, IDC Nordic



Grafen viser hvor mange penge de 13 sektorer bruger til IT-sikkerhed pr. medarbejder. Telekommunikation bruger 23.515 kr. Forsyningsvirksomhed 15.717 kr. Finans 9.511. Det offentlige 2023 kr. Metoden er en leverandøropgørelse. IDC har opdelt det i sektorer og Danmarks Statistik har leveret antal virksomheder og antal ansatte. I alt medvirker 317.000 virksomheder med 2.266.000 ansatte.

Kilde: IDC Nordic/Danmarks Statistik

FAKTA

Investeringer i IT-sikkerhed

Der bruges i alt 6,6 mia. kr. på IT-sikkerhed i Danmark. Finanssektoren bruger i alt 780 mio. kr. på eksterne leverandører. Offentlige myndigheder bruger 1,2 mia. kr. Der er 82.000 ansatte i finans, 616.000 i det offentlige. Det betyder, at det offentlige bruger under en fjerdedel på IT-sikkerhed pr. medarbejder sammenlignet med finanssektoren.

OffDig

Mød KOMBIT på OffDig 2023

Hvordan sikrer man bedre fastholdelse af ansatte i kommunerne? Hør mere når KOMBIT udfolder de seneste tendenser inden for HR.
Vi afholder efterfølgende en innovationsturnering, hvor du kan være med til at spille dig til løsninger inden for rekruttering og fastholdelse af kommunale ansatte.

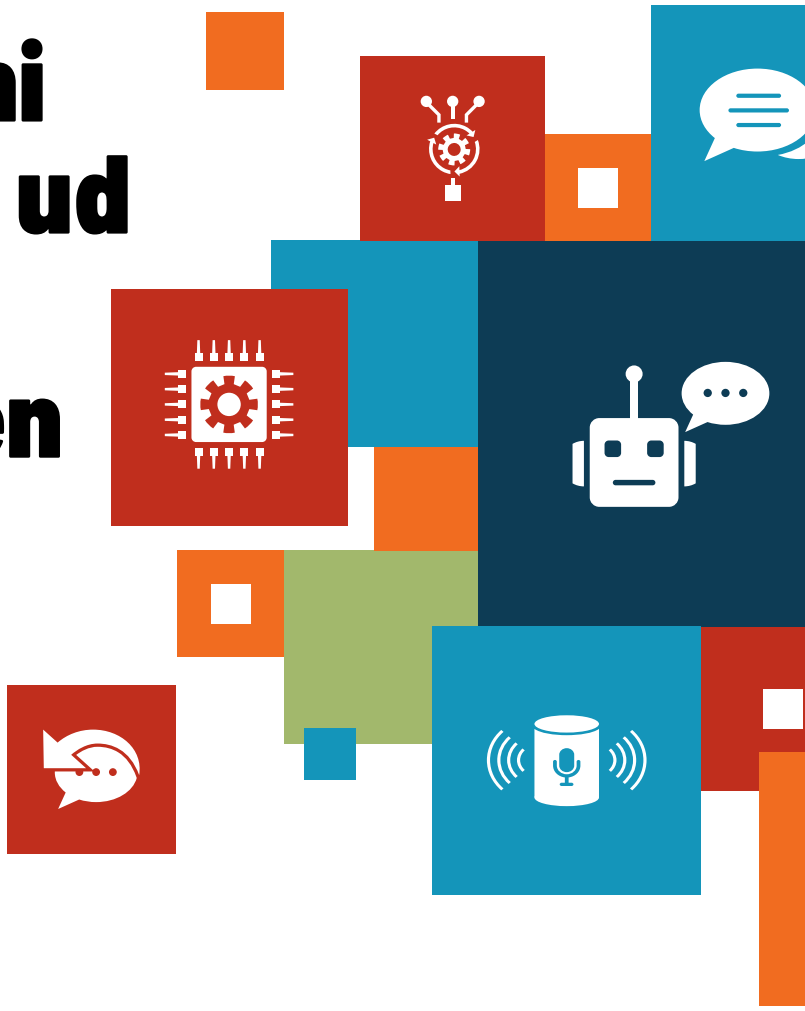
Hør også oplæg om fremtidens **åbne infrastruktur, automatiseret sagsbehandling** og om, hvordan Danmark kan **styrke sin position** som verdensledende inden for digitalisering.

Ses vi?

KOMBIT
Kommunernes it-fællesskab

Af Flemming Kjærsdam

Chatbotten Muni rækker hånden ud til borgere der bruger stemmen



Det tværkommunale fællesskab DDH (Den Digitale Hotline) har siden 2020 haft Chatbotten Muni i drift i 37 kommuner. Nu har kommunerne i fællesskab besluttet, at tiden er moden til at opgradere den kommunale Chatbots kompetencer, så den kan svare borgerne ikke alene på skrift - men også i tale. Dermed bliver Chatbotten med en Voice funktionalitet et yderligere bidrag til at få alle borgere med i det digitale samfund i Danmark.

Chatbotten Muni bliver opgraderet med Voice funktionalitet og kan servicere borgere, som ringer ind til kommunen. Indtil nu har chatbotten 5.500 indbyggede svar inden for 50 kategorier af dialoger, der kan bruges i borgerkontakten.

Formand Lene Hartig Danielsen, Den Digitale Hotline: "Jeg er optaget af, at det digitale samfund kan bruges af alle borgere. Vi skal ikke digitalisere med tvang. Her er brugen af Voice teknologien et stort spring frem, for alle som ønsker at være en del af det digitale samfund. Det er ikke alle, der kan skrive eller udfylde en formular, eller læse på en skærm, men de fleste kan godt bruge stemmen. Det er et nyt bidrag til digitaliseringen for de mange, der har udfordringer med de digitale services".

Danmark er verdens mest digitale samfund, men "en ud af tre foretrækker at ringe, hvis de har ærinder med det offentlige", siger Rambøll Rapporten IT i Praksis. Den mulighed forsvinder ikke. Voice funktionaliteten skal derimod understøtte det behov hos borgerne. Målet med projektet er at kunne udvide service og øget tilgængelighed for borgerne, så de kan få hurtigere afklaring på deres spørgsmål både i og udenfor kontaktcenterets eller kommunernes åbningstider. Den øgede tilgængelighed må dog ikke være på bekostning af kvaliteten.

Projektleder i Den Digitale Hotline Torben Glock siger: "Vi har høje ambitioner for Voice funktionaliteten, og vi tror på, at MUNI i skrift og tale samlet set kan komme til at dække 40 pct. af alle borgerhenvendelser, som DDH får i 2024. Det er dog vigtigt, at kvaliteten af den service, DDH tilbyder, fortsat er den samme. Så der er samme kvalitetskrav til Voice funktionen, som til medarbejderne i vores kontaktcenter".

Dr. Watson er IBM teknologi, som i 2021 bestod af mere end 3000 cloudservices.

"Voice funktionerne styres af kunstig intelligens. Det betyder, når en borger ringer ind, bliver han eller hun tilbudt at springe køen over, og blive betjent af chatbotten Muni. Her kan borgerne få svar på simple spørgsmål, svar om regler og kan booke en tid til et møde i jobcenteret eller hos lægen udelukkende ved at bruge sin stemme. Vi introducerer services dér, hvor borgeren naturligt bruger stemmen, og det gør man i en telefon".

"Men vi vil også åbne op for, at en borger, som bruger sin computer som telefon også vil kunne stilles igennem og få kontakt med indholdet på chatbotten oversat til lyd. Der er vi ikke endnu. Men det er næste skridt. Den tredje mulighed er at bruge chatbotten Muni som en add-on stander. Det er uden for åbningstid i Borgerservice, og her vil man kunne få svar på mange ting.

Muni har besvaret 120.000 spørgsmål fra borgerne i 2022. Muni rækker hånden ud til de borgere, der bruger stemmen.

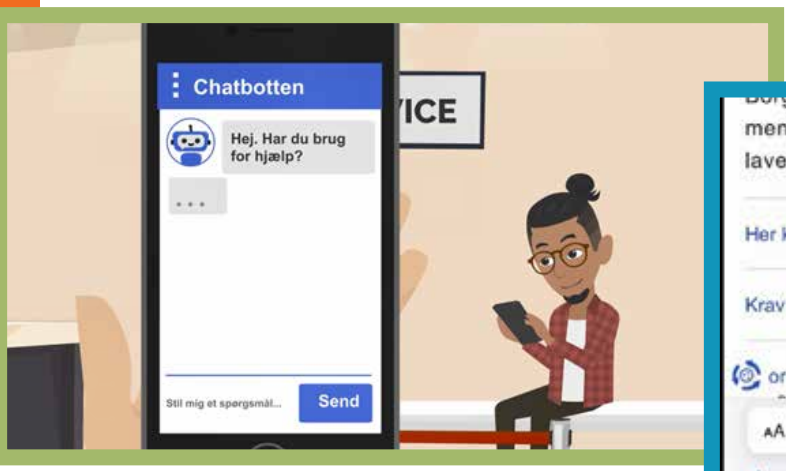
Business Casen ligger i det tværkommunale samarbejde

Ifølge Lene Hartig Danielsen viser erfaringer fra lignende projekter, at det er svært som selvstændig kommune at finde en positiv business case på Voice funktionaliteten. I DDH-fællesskabet bliver projektet dog økonomisk bæredygtigt. Det bliver nemlig muligt for kommuner at få den udvidede service i drift uden at skulle betale flere hundrede tusinde kroner, fordi alle kommuner løfter udgifterne i flok. Så business casen ligger i det tværkommunale samarbejde.

Op til 33 pct. af de danske borgere synes ikke, at det offentlige gør nok for at hjælpe dem med at bruge de digitale services. DDH blev netop sat i verden i 2012 for at hjælpe borgerne med selvbetjeningsløsninger i

Voice funktionerne styres af kunstig intelligens. Det betyder, når en borger ringer ind, bliver han eller hun tilbudt at springe køen over, og blive betjent af chatbotten Muni. Her kan borgerne få svar på simple spørgsmål, svar om regler og kan booke en tid til et møde i jobcenteret eller hos lægen udelukkende ved at bruge sin stemme.

Projektleder Torben Glock, DDH.



takt med, at det danske samfund blev mere og mere digitaliseret, og kommunerne har blandt andet gennem DDH hjulpet tusindvis af borgere, der har haft brug for hjælp til det digitale Danmark. Men borgerne har altså fortsat brug for mere hjælp. Serviceudbygningen af Chatbotten med Voice er derfor næste skridt i rejsen mod DDHs vision om at være den bedste indgang til det offentlige Danmark.

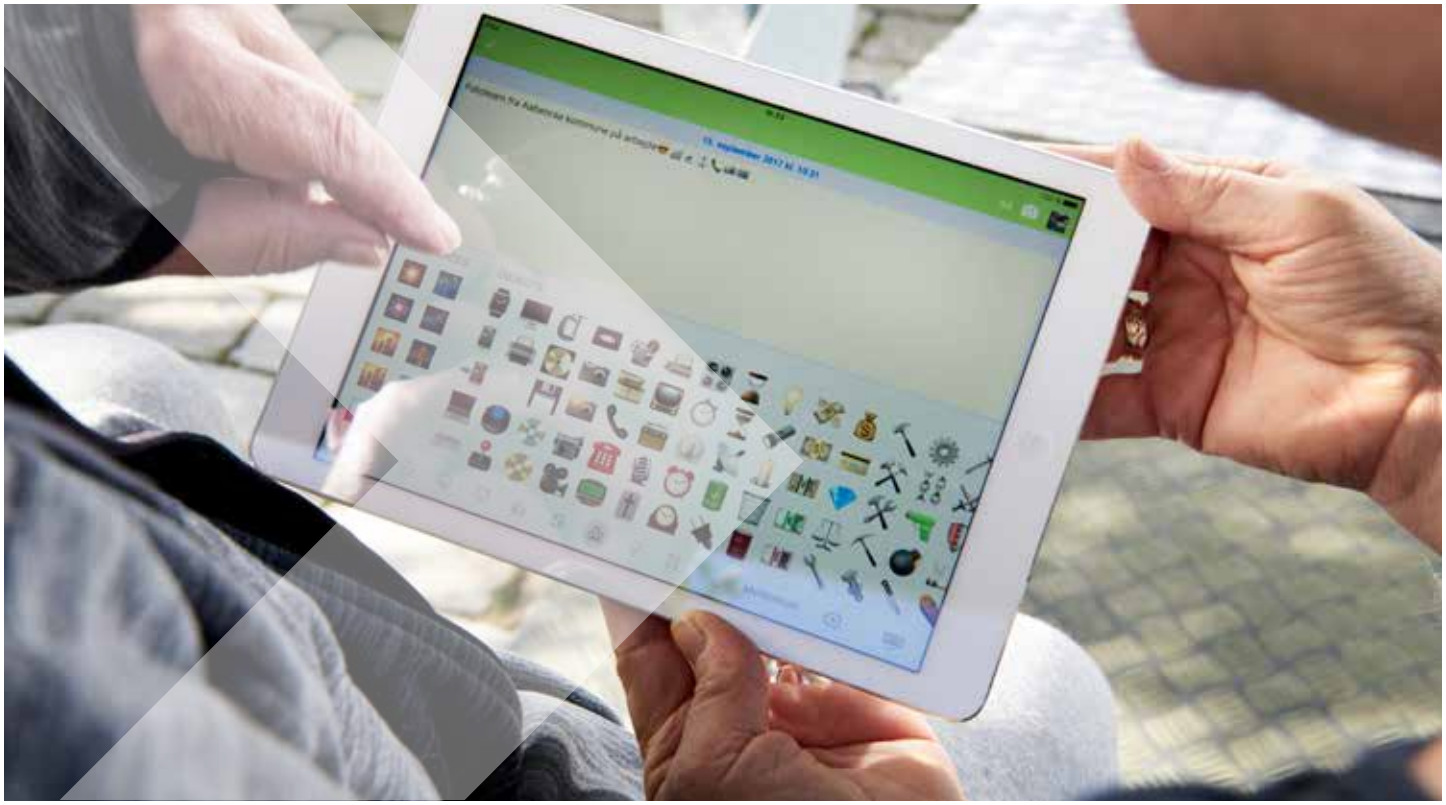
Formanden for DDH Lene Hartig Danielsen uddyber:

"Vi startede med otte kommuner i DDH for 10 år siden. Dengang havde vi ingen idé om, at vi ville indkøbe en Chatbot i fællesskab otte-10 år senere. Men det serviceniveau, som borgerne forventer af et kontaktcenter i deres kommune, ændrer sig hele tiden. Voice er startskuddet for DDH 2.0."

Jeg er optaget af, at det digitale samfund kan bruges af alle borgere. Vi skal ikke digitalisere med tvang. Her er brugen af Voice teknologien et stort spring frem for alle, som ønsker at være en del af det digitale samfund.

Formand Lene Hartig Danielsen, DDH

Af Carsten Steno



Firedobbelt bundlinje gør det nemmere at konvertere hænder til teknologi

I Aabenraa kommune har man i en årrække kortlagt en lang række digitale projekter på social- og sundhedsområdet. Samtidig har man systematisk givet politikerne indsigt i digitaliseringens muligheder. Det har skabt politisk ejerskab til stadig flere og nye digitaliseringsprojekter, der både sparer penge og forbedrer servicen overfor borgerne

Hvis kommunalpolitikere får en grundig indføring i digitaliseringen og kender dens muligheder, er det lettere at skabe forståelse for digitaliseringstiltag, der både effektiviserer og forbedrer den offentlige service.

Det vurderer Kenneth Kristensen, der i øjeblikket arbejder på en ph.d. på Syddansk Universitet om offentlig topledelse af digitalisering. Han har erfaring som direktør i fire kommuner senest som kommunaldirektør i Dragør Kommune.

Kenneth Kristensen har for KL udarbejdet rapporten - "Veje til politisk deltagelse i digitaliseringen" - og peger bl.a. på Aabenraa, som en kommune, der har arbejdet systematisk og strategisk med digitaliseringen i en årrække. Her er der en del læring af hente, men det vender vi tilbage til.

Indledningsvis peger Kenneth Kristensen på, at der skal være en vis arbejdsdeling mellem "bagbutikken", som den kommunale administration alene står for, og den del af digitaliseringen,
der vender ud mod borgerne, og som har store økonomiske konsekvenser eller involverer etiske og andre dilemmaer og derfor bør have politikernes særlige interesse.

Det administrative felt omfatter det som byrådet vælger, ikke er politisk interessant. F.eks. nye sagsbehandlings-systemer og andre administrative løsninger, som er pragmatiske tiltag, der er nødvendige, men ikke politisk relevante i anden sammenhæng end den økonomiske investering, der følger med.

De borgernære områder i fokus

De områder, der i særlig grad berører politikerne, er de borgernære områder, hvor digitaliseringen kan frigøre ressourcer og i mange tilfælde også forbedre servicen for borgerne. Hvis digitaliseringen f.eks. vedrører en robot, der kan bespise et handicappet barn, eller intelligente bleer, der bruges i hjemmeplejen, er det afgørende, at politikere har sat sig ind i teknologien, kender dens muligheder og kan forklare og forsvare tiltaget overfor borgerne. Eller omvendt måske standse en digitalisering, der hvor den ikke opleves som hensigtsmæssig i forhold til borgeren.

I Aabenraa kommune har byrådet på social- og sundhedsområdet vedtaget en strategi og en handleplan med tilhørende anlægsmidler til digital sundhed- og velfærdsteknologi på baggrund af businessca-

ses, hvor den efterfølgende drift skal finansiere sig selv. Området er ikke en politisk kampplads, for der er enighed i byrådet om strategien og dermed det politiske ejerskab til den.
Strategien har fire bundlinjer. Den skal frigøre ressourcer, gøre borgerne mere selvhjulpne, bidrage til at fastholde medarbejdere og i samarbejde med lokale leverandører skabe vækst og nye arbejdspladser i kommunen.

Politikerne skal have indsigt i digitalisering

De mål mener Kenneth Kristensen godt kan indfries forudsat, at man som i Aabenraa har gjort en stor indsats for at engagere byrådsmedlemmerne og give dem indsigt i, hvad digitalisering er og kan bruges til. I Aabenraa har man arbejdet strategisk med digitalisering siden 2009 – først ud fra økonomiske hensyn, men senere ud fra den firedobbelte bundlinje, som i øvrigt nu også omfatter bæredygtighed.
"Uddannelsen" af politikerne i digitalisering omfatter bl.a. workshops, hvor politikerne selv afprøver forskellige digitaliseringsløsninger, demonstrationer, institutionsbesøg, og besøg hos leverandører. Uddannelsen omfatter også studierejser, f.eks. en studietur til Holland, hvor man arbejder med digitaliseringen på samme vis som i danske kommuner.
At politikernes engagement og viden om digitalisering rent faktisk gør en forskel bekræfter direktøren for kommunens social- og sundhedsområde, Karin Storgaard Larsen. Hendes forvaltning har løbende ca. 50 borgernære digitaliseringsprojekter i gang, hvoraf ca. halvdelen sættes i drift efter beslutning i social og seniorudvalget. Siden 2017 har udvalget årligt godkendt en projektplan, hvor de digitaliseringsløsninger, der arbejdes med, præsenteres for udvalget som i mange tilfælde også selv får mulighed for at afprøve dem.

Politisk ejerskab er afgørende

"Processen giver politisk ejerskab og politisk vilje til digitalisering og teknologiudvikling på et helt andet niveau, end hvis man arbejder med digitaliseringen i et tværgående udvalg, hvor det er langt fra den daglige drift", siger Karen Storgaard Larsen
Anledningen til at man i Social- og Sundhedsforvaltningen ændrede sin tilgang til digitalisering og besluttede sig for at afprøve digitale løsninger i større omfang, var oprindelig den såkaldte "robotstøvsuger-debat", hvis omdrejningspunkt var om robotstøvsugere i praksis kunne erstatte en medarbejder, der kom ud for at støvsuge. Debatten kørte uden at man havde lavet forsøgsprojekter, der kunne give et bedre beslutningsgrundlag.
"Nu afprøver vi en lang række teknologiske løsninger på velfærdsområdet og vurderer om de virker, før vi sender dem i drift", fortæller Karen Storgaard Larsen.
Det kan f.eks. være genoptræningsprogrammer for borgere, der har været indlagt, eller det kan være "skærmbesøg", der erstatter indsatser, som tidligere har været løst ved at sende en medarbejder ud.
Karen Storgaard Larsen oplyser, at de hidtidige digitale løsninger i mange tilfælde har suppleret det, som medarbejderne har kunnet gøre ude hos borgeren, hvorved der samlet set er opnået en bedre effekt. Men de nye muligheder har samtidig affødt større forventninger hos borgerne til den service de får.
Derimod har tiltagene ikke nødvendigvis reduceret antallet af personkontakt-minutter, som der er brug for ude hos borgere.

Konvertering af hænder til teknologi

Det betyder dog ikke nødvendigvis, at projekterne ikke har ført til besparelser. Når digitaliseringsløsningerne går fra projektstadiet til drift, skal den enkelte enhed nemlig som udgangspunkt finansiere løsningen indenfor sit driftsbudget. Og det kan betyde, at udgifter til f.eks. skærme ude hos borgere og licenser må finansieres ved at reducere i lønbudgettet i forventning om at løsningen har reduceret arbejdsopgaven for medarbejderne.

FAKTA

Erfaringer fra Aabenraa

- **Skab bredt politisk ejerskab, så fejl ikke bliver en politisk kampplads**
- **Brug handleplaner og resultatopgørelser**
- **Skab risikovilje til nye projekter ved at give politikerne indsigt.**
- **Lad politikerne selv afprøve de digitale løsninger.**
- **Lad være med at formulere digitaliseringsprojekter som rene besparelsesprojekter**

I 2023 er det aftalt med Social og Seniorudvalget, at der i højere grad afprøves digitale løsninger, som konverterer "hænder til teknologi". Det er afledt af den vanskelige rekrutteringssituation.
"Tidligere var sådanne tiltag ikke populære, fordi medarbejderne frygtede at blive afskediget. I dag, hvor det kniber at rekruttere, har holdningen ændret sig. Nu vil medarbejderne gerne være med til at afprøve teknologier, som kan aflaste for nogle af de opgaver, som de løser i dag", siger Karen Storgaard Larsen.
Som eksempel på en mulig digital løsning, der kan konverteres hænder til teknologi, nævner Karen Storgaard Larsen håndtering af nødkald, som er meget ressourcekrævende. Nødkald går i dag via en vagtcentral, som vurderer om en medarbejder skal sendes ud.
"Men hvis vi f.eks. havde adgang til et videokamera i hjemmet, ville vi bedre kunne vurdere om der er behov for at sende medarbejdere ud. Det kunne vi godt køre et forsøg med, men det støder dog på lovgivningen, som ikke umiddelbart tillader videooovervågning i et hjem, heller ikke selvom borgeren giver sin tilladelse".

"I 2023 er det aftalt med Social og Seniorudvalget, at der i højere grad afprøves digitale løsninger, som konverterer "hænder til teknologi". Det er afledt af den vanskelige rekrutterings-situation. Tidligere var sådanne tiltag ikke populære, fordi medarbejderne frygtede at blive afskediget. I dag, hvor det kniber at rekruttere, har holdningen ændret sig. Nu vil medarbejderne gerne være med til at afprøve teknologier, som kan aflaste for nogle af de opgaver, som de løser i dag.
Karen Storgaard Larsen, Aabenraa Kommune.

Af Flemming Kjærsdam

Kristian Vengsgaard, KOMBIT:

"Lampen lyser rødt med rød på"

Cybersikkerheden og beskyttelsen mod udefrakommende cyberangreb er desværre mere aktuel end nogensinde før. "Det er jo sådan, at Center for Cybersikkerheds risikovurdering er rød. Eller den er rød med rød på. Det kan næsten ikke blive værre," siger CEO Kristian Vengsgaard, KOMBIT, som har overtaget stolen efter Thomas Rysgaard Christiansen.

Da Kristian Vengsgaard overtog jobbet efter Thomas Rysgaard Christiansen, hed det sig, at han skulle kunne sætte sit aftryk på den nye KOMBIT strategi. Men begivenhederne omkring KOMBIT har haft så meget fart på, at han tøver en kende med strategien og gerne vil tage kommunerne med på råd en ekstra gang.

"KOMBIT blev sat i verden for at gennemføre Monopolbruddet. Det har vi afsluttet. Men vi har fortsat en stor opgave med at sikre, at den nye portefølje af løsninger, vi har indkøbt til kommunerne, kører optimalt og løbende bliver videreudviklet og fornyet. Og så er der kommet nye opgaver oveni. Så strategien kommer ikke til at skifte radikalt. Jeg tror den mulighed, vi står overfor nu, er, at vi kan dreje skarpere. Det betyder ikke, at vi skal dreje væk fra det, vi laver i dag. Men måske skal vi udvide vejbanen nu, hvor monopolbruddet er gennemført, og vi, med det store arbejde der er lagt i det, har skabt et meget stærkt fundament for KOMBITs fremtidige virke".

"Vi skal fortsat levere nogle ordentlige udbud i høj kvalitet og sørge for, at få leverandørerne animeret til den type initiativer, som i høj grad har med den gamle kerneforretning at gøre, og som fastholder konkurrencen på markedet. Men strategiprocessen giver også nogle nye muligheder, hvor eksempelvis KOMBITs implementeringsmandat bør komme til et eftersyn. Det er vi interesseret i, og det ved jeg også, at kommunerne er. Vi må jo erkende at "leverancer til

kantstenen" ikke altid er tilstrækkeligt for alle 98 kommuner – måske skal der hjælp til at installere vaskemaskinen de steder, hvor man ikke lige har en vvs-installatør i familien".
"I og med der kom et direktørskifte midt i strategiarbejdet, bad jeg og bestyrelsen i fællesskab om at få lov til at trække strategien en smule. Kunne vi sammen med kommunerne kigge på den igen? Det er så det, vi er i gang med nu. Vi har fået et mandat fra bestyrelsen til at undersøge, om vi kan gå endnu længere og endnu bredere ud med de opgaver, vi løser for kommunerne. Derfor tager vi en ekstra runde med kommunerne og sender en spørgeskemaundersøgelse ud, hvor vi spørger ind til, hvad de vil bruge KOMBIT til. Hvad kan vi gøre for dem? siger Kristian Vengsgaard.
Undersøgelsen skal give KOMBIT et dybere indblik i, hvilke forventninger kommunerne har, men også hvor kommunerne har udfordringer i forhold til kompetencer, demografi, brugen af data, cybersikkerhed, grøn omstilling og digitaliserings understøttelse generelt.

Tre udfordringer

Kommunerne står over for en økonomisk udfordring på socialområdet. Kristian Vengsgaard omtaler det som den "nationaløkonomiske hængekøje". Der er mange unge og mange ældre, som udfordrer kommunernes økonomi, og der er mangel på arbejdskraft.
"Økonomien i kommunerne er presset. Vi kigger ind i en periode, hvor forholdet mellem skatteindtægter og arbejdsudbud ikke følges ad. Det bliver bedre om 10-15 år. Men vi får en periode, hvor vi både mangler penge og mangler arbejdskraft. Og hvor der skal bruges mange penge på børn og ældre. Seks ud af 10 offentligt ansatte er ansat i kommunerne, så den her hængekøje rammer det kommunale landskab hårdt".
"Udover en presset økonomi og store udfordringer i forhold til bæredygtighed og den grønne omstilling, så er der også den forandrede sikkerhedssituation i Europa. Set med it-øjne er det cybersecurity - og hele den front er desværre mere aktuel end nogensinde. Lampen lyser rødt med rød på. Den situation kan desværre ikke blive værre. Jeg kender til det fra min tid i Forsvaret".

I Danmark har de seneste uger vist farligheden af disse cyberangreb
"Det er en problemstilling, som kommunerne møder dagligt og som vi, set med mine øjne, er nødt til at tage os af. Men hvad gør vi, hvis en kommunes data bliver taget til fange i et ransomware angreb? Vi ved jo nok ikke helt præcist, hvad vi skal stille op. Hvordan kan vi nationalt og lokalt med cyberangreb tage hånd om det? Hvad gør politiet efterforskningsmæssigt? Det er nogle udfordringer, som er nye på den måde, at de er større, og de er mere præsente end nogensinde før. På den anden side er det jo noget, vi hele tiden har vidst, vi skulle have fokus på."

- fortsættes på side 16 »»»

"For nogle er sikkerhed en sten i skoen. For mig er sikkerhed forretning - og beskyttelse af data og driften kerneforretningen.

Kristian Vengsgaard, KOMBIT.

"Lampen lyser rødt med rød på"

"Der foregår både statslige aktiviteter og kriminelle aktiviteter. Cyberangreb - og cyberaktiviteter i det hele taget - er blevet industrialiseret. Det er blevet en hel industri og rent økonomisk en gigant industri. Både fordi staterne putter rigtig mange penge i det og fordi, at de organiserede kriminelle også putter rigtig mange penge i det. Og problemet er, at de bruger de mest moderne værktøjer i verden. Vi kan se, at nogle af de angreb, vi ser i virkeligheden, er relativt lavpandede og sådan lidt stenalderagtige, men det kan jo være, fordi vi ikke ser dem alle," siger Kristian Vengsgaard.

Konsolidering og færre angrebsflader

Kristian Vengsgaard: "Ja, man kan i hvert fald sige, at en løsning på cyberudfordringer altid er teknisk konsolidering. Det er altid at skære i antallet af angrebsflader. Cybersikkerhedsfolk kalder det angrebsvektorer. Når man har en meget bred portefølje af systemer af teknik, og her taler vi jo telefoner, netværk, switche, servere i kælderen, skabe med data, wifi spots, ting der kan opsamle informationer i væggene, kameraer. Alt, hvad der er elektronisk, udgør i realiteten en angrebsvektor. Jo flere desto mere sårbar".

"Et stort forsvarsministerium blev engang angrebet gennem en mikrobølgeovn, fordi de havde besluttet sig for, at den skulle på nettet, så de kunne downloade nogle opskrifter til den der mikroovn. Det eneste de brugte den til var at lave popcorn. Men der er eksempler på, at Jeeps biler er blevet overtaget, mens de kørte på motorvejen."

"Desværre er det simplere at lave disse hackerangreb, end man skulle tro. Selvom man har et godt setup, selvom man har beskyttet sig rigtig godt, så hvis hackeren har tid nok, og man har adgang, så kan man komme langt. Det foreløbige kendskab, jeg har nået at få til kommunernes cybersikkerhed, er jo relativt begrænset. Men det landskab, som jeg tror kommunerne har på det her område, er præget af mange forskellige aktører og leverandører og er i bedste fald meget komplekst.

"Det handler om at kunne styre, hvem er på netværket? Hvad laver de på netværket? Hvad er det for nogle enheder, der er på netværket, og hvordan er de enheder beskyttet? Hvis man virkelig vil have styr på sikkerheden, så skal man have styr på alle de enheder, og det kalder på nye måder at anskue det på"

"Man kan som minimum sige, at cybersikkerhed kalder på teknisk centralisering. Du er nødt til at kunne opstille nogle rammer for, hvad man må, og hvad man ikke må. Vores servere og netværk skal segmenteres. Vores telefoner skal være underlagt MDM (Mobile Device Management), så vi kan styre dem. Det er den type ting, Center for Cybersikkerhed sender anbefalinger ud om. I øjeblikket er der 38".

"For nogle er sikkerhed en sten i skoen. For mig er sikkerhed forretning - og beskyttelse af data og driftener kerneforretningen," siger Kristian Vengsgaard

«««

"Udover en presset økonomi og store udfordringer i forhold til bæredygtighed og den grønne omstilling, så er der også den forandrede sikkerhedssituation i Europa. Set med it-øjne er det cybersecurity - og hele den front er desværre mere aktuel end nogensinde. Lampen lyser rødt med rød på. Den situation kan desværre ikke blive værre. Jeg kender til det fra min tid i Forsvaret.

CEO Kristian Vengsgaard, KOMBIT.

Sikring af ledelsestilsynet kom med standard IDM-løsning i Langelands Kommune

Målene var klare, da Langelands Kommune valgte en løsning fra ID Connect til at digitalisere kommunens brugeradministration. Ledelsestilsynet skulle opfyldes, det skulle være markant lettere for lederne at håndtere brugerstyring, og samtidig skulle kommunens dokumentation være effektiv og sikker.

En tryg forbindelse mellem medarbejdere og kommunale services
I Langelands Kommune er det Rikke Birgitte Grube, der er ansvarlig for implementeringen af ID Connects brugerstyringsløsning, som lige nu er ved at blive rullet ud til alle kommunens forretningsområder.

- Vi har kun været i gang i siden foråret 2022, men vi oplever allerede, at der er markant bedre styr på håndteringen af vores brugere. Den automatiserede løsning har både gjort det lettere for vores ledere, og samtidig er sikkerheden i top, forklarer Rikke Grube.

Foto: Mette Johnsen

Sådan kom Langelands Kommune i gang
- Da vi begyndte at afdække markedet i forhold til understøttelse af brugerstyring, lagde vi vægt på, at leverandøren skulle have indgående kendskab til det kommunale marked og samtidig have en let tilgængelig løsning, som også kunne betales for en lille kommune. Dette har vi til fulde fået med ID Connect, siger Steen Bihl Nielsen, som er leder af Økonomi og Indkøb.

Ved brug af bl.a. referencetjek stod det klart, at løsningen passede godt til kommunens ønske om, at kommunen skulle leve op til ledelsestilsynet. Herefter var det Rikke Grube, der fik ansvar for at implementere løsningen.

- Der er helt basalt taget rigtig godt imod løsningen i vores organisation, men fordelene er også til at få øje på. ID Connects løsning kræver oplæring af lederne, men så snart de oplever, hvor hurtigt og nemt det går – uanset om der er tale om oprettelser eller nedlukninger af brugere – så er de med ombord, forklarer Rikke Grube, og fortsætter:

- Derudover har det virket godt for os, at vi kender alle 'byggestenene' i løsningen, og så har vi selv været med til at sætte dem sammen på en måde, som giver størst mulig gevinst for os – selvom der er tale om en standardløsning. Vi lever fint med, at ID Connect har en fast ramme, fordi det tvinger os til at tage stilling.

Fra Servicedesk til selvhjælp
Tidligere skulle lederne omkring kommunens Servicedesk for oprettelse af nye brugere og for eventuelle spørgsmål. Med den ny løsning spares der tid i begge ender.

- Når lederne er onboardet, kan de tilgå alt i løsningen med det samme. For den enkelte leder betyder det, at fx en ny medarbejder eller en vikar kan gå i gang med arbejdet med det samme. Deres rettigheder og adgange er oprettet lynhurtigt, og al spildtid er skåret væk, siger Rikke Grube.

Udover tidsbesparelsen, så oplever Rikke Grube også mindre frustration.
- Vi har selv indkøbt løsningen, og det betyder, at vi følger den plan, vi har vedtaget. Med andre ord, så har vi valgt at gå automatiseringens vej, og den vej fortsætter vi hen ad,

Langelands Kommune har i dag fået en sammenhængende proces, hvor gevinstrealiseringen er højnelse af sikkerheden og frigivelse af ressourcer i organisationen.

- Jeg kan slet ikke se, hvordan en kommune – uanset om den er stor eller lille – kan styre deres brugere uden en digital løsning i dag, siger Rikke Grube.

Involvering har været nøglen
Med stor opbakning fra ledelsen i Langelands Kommune er implementeringen af ID Connect-løsningen i organisationen gået godt.
Processen har involveret alle ledere, der indledningsvist deltog i et ID Connect-foredrag om løsningen. Efterfølgende har Rikke Grube gennemgået alle detaljer i løsningen med hver enkelt leder, så de i dag kender løsningen og dens muligheder til bunds. Det er med til at sikre en ensartet brug af løsningen.
- Det er bl.a. kommet til udtryk ved vores seneste organisationsændring. I vores verden kan disse ændringer komme hurtigt og i flere omgange, og her må jeg sige, at ID Connect-løsningen sikrer, at fejl i håndteringen af vores brugere er fjernet. Vi har nu en proces, som er let og ubesværet, forklarer Rikke Grube.

Rikke Grube fortæller, at netop organisationsændringer påvirker bredt i en kommune, så også kommunens systemer påvirkes.

- Netop ved organisationsændringer spiller tildelingen af rettigheder en stor rolle. Her hjælper de rapporter, der er en del af ID Connect-løsningen, os ved at vise alle eksisterende roller og er dermed med til at øge vores sikkerhed. Vi har simpelthen både overblik, gennemsigtighed og høj sikkerhed, siger Rikke Grube.

Samarbejdet med ID Connect
Rikke Grube påpeger, at samarbejdet med ID Connect har været intet mindre end fantastisk og præget af god dialog, hurtig respons og solid rådgivning.

- Jeg vil til enhver tid sige, at samarbejdet med en leverandør er væsentligt, og servicen er der jo styr på. I Langelands Kommune føler vi, at vi bevæger os fremad sammen med ID Connect.

- ID Connect er grundstenen, der løfter Langeland Kommunes brugerstyringsstrategi. En strategi, hvor det er den brugeransvarlige leder, der selv tildeler de rettigheder, som den enkelte bruger har behov for i sin opgaveløsning, slutter Mikael Kronstrøm, der er leder af Digitalisering og IT.

Læs mere på www.idconnect.dk

id connect

Af Flemming Kjærsdam

EU-parlamentsmedlem Morten Løkkegaard (V):

"Cybertruslen har fået enorm bevågenhed i alle EU-lande"

Det er meget sjældent at opleve, hvordan alle stater, kommuner og erhvervsliv rykker samtidig på et emne. Det er cybertruslen, der er emnet. Der er stor enighed i alle led. Og cybertruslen har fået enorm politisk og økonomisk bevågenhed. Det siger EU-parlamentariker, Morten Løkkegaard (V), der også sidder i Gentofte Kommunes byråd.

EU-parlamentariker Morten Løkkegaard siger, at det er meget længe siden, han har oplevet et tilsvarende ryk i opmærksomhed som cybertruslen har skabt i 27 EU-lande. Det sker i alle led. Både i nationalstaterne, centraladministrationerne, kommunerne og erhvervslivet "er cybertruslen det altoverskyggende emne", som suger opmærksomheden til sig.
"Det er ingen overraskelse for mig, men det er fascinerende at opleve det ryk, der sker. Det kører løs nu, men den gode nyhed er også, at kredsen af lande, der er gået i gang med implementeringen af NIS2-direktivet synes bredere end den plejer. Så man kan godt sige, at på det politiske niveau, altså på statsniveau, da virker det som om, at der er kommet skred i tingene. Ganske enkelt fordi sikkerhedspolitik fylder så meget i alle led og i alle europæiske hovedstæder. Og derfor er det også helt klart min forventning, at implementeringen vil være anderledes, mere effektiv og hurtigere end den plejer," Morten Løkkegaard.
I PwC´s Cybercrime Survey 2022 siger 59 pct. af topledere, at de forventer, at de vil øge investeringerne i it-sikkerhed i 2023.
"Jeg tror snarere, at tallet er lidt for lavt sat. Vi befinder os midt i en bølge og jeg forventer, at det vil blive endnu større efterhånden som truslen vokser," siger Morten Løkkegaard.

Indbakken er fyldt

Ikke nok med at cybertruslen har stor bevågenhed blandt politikere og embedsmænd. Det har det også i erhvervslivet og i kommunerne. På et mere jordnært niveau, er Morten Løkkegaards indbakke stopfyldt med henvendelser.
"Det er helt vildt så mange mails og telefonopkald, som kommer ind på mit kontor, og som udelukkende handler om cybertruslerne. Det er uomtvisteligt, at der foregår rigtigt meget i virksomhederne, men kommunerne er også ved at komme med. Hvis jeg skal vurdere på antallet af henvendelser, så er det i hvert fald seks år siden, jeg har oplevet noget tilsvarende med en lovgivning, der optog sindene på den måde. Og trykket er større idag. Man kan mærke, at en hel branche, ja, et helt erhvervsliv sætter sig i bevægelse og stort set alle lande i unionen rykker med. Det har så sat sig i NIS2-direktivet, fordi lovgivningen er karakteriseret ved, at alle skal med. Så det jo ikke kun er virksomhederne, men også centraladministrationerne, der er optaget af det, og jeg kan mærke, at kommunerne begynder at rykke," siger Morten Løkkegaard.

NIS2 er kun et første skridt

Cybertruslen er også begyndelsen til en ny virkelighed. Kommuner og virksomheder skal opbygge et beredskab, der beskytter data, mennesker og bygninger og anlæg. Men NIS2 adresserer ikke manglen på kompetencer og uddannelse og rekruttering af arbejdskraft. Alle niveauer og instanser kommer til at mangle kvalificeret arbejdskraft.

Inden for de seneste par uger har finansministrene i EU-landene (Ecofin) været samlet for at drøfte den situation.

"EU-Kommissionen er udmærket klar over problemets omfang, og vi taler om milliardinvesteringer for at løse de udfordringer i fremtiden, som betyder mere uddannelse og rekruttering, der fører til en ny industriel politik. Det er jo en ny stor indsats, som foregår på allerøverste politiske niveau. For at give NIS2-direktivet en effekt, er du nødt til at uddanne mennesker og skaffe arbejdskraft. Der er mangel på eksperter internt i virksomheder og organisationer".

Kommunerne skal med i NIS2

Foruden NIS2 kommer Cyber Resilience Act, (CRA) som er en lovgivning, der fokuserer på digitale produkter, der er koblet på internettet – alt fra køleskabe, sensorer på fabriksrobotter og biler.

Morten Løkkegaard forventer, at han kommer med i med i arbejdet om den nye CRA.

"Uanset hvordan du kigger på det, så har NIS2 og cybertruslen høj politisk prioritet. Det er på grund af de milliardinvesteringer, der skal gøres nu til vores forsvar og på den Industrielle del og det offentlige. Når vi snakker klimainvesteringer hænger det uløseligt sammen, med digitalisering og IT-sikkerhed," siger Morten Løkkegaard.

"Jeg er optaget af, at det både kan fungere kommercielt og politisk. Det bliver kun mere aktuelt og mere vigtigt for hver dag der går, og at vi får taget hånd om hele paletten, så vi kan være med på alle niveauer i EU".

"Det er ingen overraskelse for mig, men det er fascinerende at opleve det ryk, der sker. Det kører løs nu, men den gode nyhed er også, at kredsen af lande, der er gået i gang med implementeringen af NIS2-direktivet synes bredere end den plejer. Så man kan godt sige, at på det politiske niveau, altså på statsniveau, da virker det som om, at der er kommet skred i tingene.

EU-parlamentsmedlem Morten Løkkegaard (V)

"Dem, jeg snakker med i kommunerne, især i Gentofte, de siger, at der ikke er nogen vej udenom. De er nødt til at komme med i NIS2. Truslen vokser, så de rykker nu. NIS2 kommer nok for sent til, at det kan blive en del af dette års kommuneaftale. Men i Gentofte investerer de en hulens masse penge på digital udvikling og opkvalificering af medarbejdere og udstyr og IT-sikkerhed. Uagtet at kommunerne endnu ikke er omfattet af NIS2, så har de indset nødvendigheden af beredskabet. De investeringer de foretager på området er den største post overhovedet på kommunens nye budget i de kommende år, så man kan sige, at nogle kommuner har fanget budskabet, hvis man har dygtige medarbejdere, der er optaget af dette emne, siger Morten Løkkegaard.

Af Flemming Kjærsdam

PwC: Seks ud af 10 investerer mere i cybersikkehed

Virksomheder og offentlige myndigheder skal forberede sig på, at risikoen for at blive ramt af et cyberangreb fra kriminelle bliver til stadighed større. Det siger direktør Mads Nørgaard Madsen, teknologi og sikkerhed i PwC. 59 pct. af alle CXO'er og it-fagfolk forventer således, at deres virksomheds cyber- og informationssikkerhedsbudget vil vokse inden for de næste 12 måneder. Det fremgår af PwC´s årlige survey inden for cyberkriminalitet 2022.

51 pct. af de danske CXO'er og it-fagfolk svarer i undersøgelsen, at deres virksomhed eller organisation har været udsat for mindst én sikkerhedshændelse inden for det seneste regnskabsår. Trods et mindre fald i forhold til 2021 er det fjerde år i træk, at mere end hver anden har været ramt.
Det er den perfekte storm for en sikkerhedsrådgiver. Virksomhederne bruger flere penge på at beskytte sig og de kriminelle arbejder sammen om at foretage angreb på it-organisationerne.
"Årsagen til den stigende cybertrussel, er, at man i takt med den omfattende digitalisering, virksomheder og it-organsiationer har undergået, ikke i tilstrækkelig grad har tænkt sikkerhed ind. Der gøres et godt stykke arbejde, men truslerne vokser. Derfor er det positivt, at næsten 60 pct. af virksomhederne vil investere mere. Der er jo mange, der allerede investerer i forvejen. Det er jo ikke fordi, folk har siddet på deres hænder og lavet ingenting. Der er jo rigtig mange, der har knoklet med sikkerhed og med at gøre mere for at mindske cyberrisikoen. Mange organisationer er dog ikke i mål, og de må konstatere, at de er nødt til at investere endnu mere for at komme helt i mål med deres cybersikkerhed. Og det vælger jeg at tolke positivt," siger Mads Nørgaard Madsen.

Ny regulering

Udover at ledelsen i private virksomheder og offentlige myndigheder skal beskytte sig endnu bedre mod udefrakommende cybertrusler, skal de også leve op til ny regulering på området. I kølvandet på GDPR-forordningen fra 2018, har EU-kommisionen vedtaget direktivet NIS2, som er en opfølgning "mod cyberangreb på kritisk infrastruktur".
Endnu er det ikke vedtaget af Folketinget, hvorvidt kommunerne bliver en

del af NIS2-direktivet, men Mads Nørgaard Madsen mener, at der ikke kan herske tvivl om, at kommunerne bliver omfattet, da de sidder på store dele af den samfundskritiske infrastruktur, som el- vand- og varmeforsyning, kommunal hjemmepleje og opsamling af skrald.

"NIS2-direktivet vil udvide kravene til cybersikkerhed og sanktionerne ved manglende overholdelse af dem for at harmonisere og strømline sikkerhedsniveauet på tværs af medlemslandene. Det medfører skærpede krav til flere sektorer og betyder, at virksomhederne og offentlige organisationer skal forholde sig til risikostyring, kontrol og tilsyn".

"Vi ser også, at flere virksomheder ønsker at arbejde mere helhedsorienteret med cybersikkerhed. Men det er samtidig vores erfaring, at en væsentlig andel af virksomhederne ikke får implementeret vedvarende programmer for håndtering af sikkerhed."

"Man kan sige, at GDPR på nogle områder virkede. Der er dog også eksempler på, at man slet ikke er i mål. Mit råd er, at ledelser i kommuner og virksomheder skal binde GDPR sammen med NIS2 og cybertruslen. I dag er mange organisationer og virksomheder kun nået til første bølge, som er alt det juridiske med databehandleraftaler og Schrems II-afgørelsen. Man mangler dog fortsat alt det svære. Jeg anbefaler, at man ser aktiviteterne under GDPR, NIS2 og cybertruslen under ét, da de alle peger på det samme. Du skal have styr på din forretning. Du skal vide, hvor dine data er, og at de er beskyttede. Ved at slå aktiviteterne sammen, kan man slå mange fluer med et smæk," siger Mads Nørgaard Madsen.

Ledelsesansvar

At have styr på forretningen er kernen i det setup, virksomheder og kommuner skal igennem. Der er et helt selvstændigt topledelsesansvar i NIS2 direktivet.

"Topledelser kan ikke bede IT-afdelingen om at tage ansvaret for forretningen. Du kan bede IT-afdelingen om hjælp til at løse det, hvis en kommune er blevet angrebet. I øvrigt har sikkerhedsagendaen sat en fornyet dialog i gang i topledelsen om et beredskab. Et beredskab om, hvordan forretningen kommer op at køre igen, efter den er blevet ramt. Det er ikke IT-afdelingens ansvar. Det er topledelsens ansvar, fordi det handler om forretningsprocesser."

"Hvis en kommune har fået sit netværk lagt ned, kan man så undervise i folkeskolen uden brug af netværk og computere? Det skal man som minimum vide, om man kan. Kan hjemmepelejen komme ud og besøge ældre i eget hjem uden adgang til data? Det er ikke IT-afdelingens ansvar. Det kræver beredskabsplaner, og det er en interessant vinkel. Ja, men IT-afdelingen har backup, siger ledelsen. Det skal de nok fixe, bare rolig. Det er alle disse workarounds, man skal være forberedt på. Det er forbundet med et ledelsesansvar. Og hvis man ikke påtager sig det, risikerer man at få bøder i en helt ny størrelsesorden," siger Mads Nørgaard Madsen.

Trusselsbilledet

I PwC´s survey svarer topledere, at de er mest bekymrede for at blive ofre for de kriminelle bander. Tidligere var truslen at hackerne kom indefra. Det er ikke tilfældet idag, da kriminelle bander forsøger at lokke medarbejderne i virksomheder og organisationer til at begå en fejl. Det kan være et klik på et link i en mail eller udlevering af et password, og så har man balladen.

"De lokker medarbejderne til at gøre noget, de ikke skulle gøre, eller siger de skal reparere radiatoren nede i kælderen, og så åbner de dørene for de kriminelle, og så er de inde. Det er sikkerhedsmæssigt et svagt led. Der skal blot være en medarbejder, der gør fejl, så har vi balladen"

Den viser, at der er meget lille tillid til kommunerne - dvs. blandt alle folk der har deltaget, har de angivet at der er lille tillid til kommunernes "evne" til at beskytte data.

Den siger ikke om de reelt er dårligere, men at opfattelsen af deres styrke på området ikke er god.

"Jeg anbefaler, at man ser aktiviteterne under GDPR, NIS2 og cybertruslen under ét, da de alle peger på det samme. Du skal have styr på din forretning. Du skal vide, hvor dine data er, og at de er beskyttede. Ved at slå aktiviteterne sammen, kan man slå mange fluer med et smæk.

Direktør teknologi og sikkerhed, Mads Nørgaard, PwC

Cybercrime Survey 2022

73 %

af CXO'er og it-fagfolk angiver, at deres øgede bekymring for cybertrusler i nogen eller i høj grad skyldes konflikten mellem Rusland og Vesten.

47 %

regner hacktivister blandt de største trusler. Det er 11 %-point flere end sidste år og den største andel nogensinde.

51 %

angiver, at deres virksomhed har været udsat for mindst én sikkerhedshændelse inden for det seneste regnskabsår. Det er fjerde år i træk, at mere end hver anden virksomhed har været ramt.

For så vidt angår tilliden til cybersikkerhed, er billedet stort set uændret i forhold til 2021. Der er fortsat størst tillid til cybersikkerheden i den finansielle sektor, hvor hele 89 % angiver, at de i nogen eller i høj grad har tillid til cybersikkerheden (90 % i 2021). Tilliden til kommunernes niveau af cybersikkerhed er ligesom i de forgangne år lavest sammenlignet med øvrige sektorer, idet 31 % angiver, at de i nogen eller i høj grad har tillid til denne sektors niveau af cybersikkerhed (30 % i 2021). Næsten halvdelen (46 %) angiver, at de i mindre grad har tillid til kommunernes niveau af cybersikkerhed, mens en femtedel ingen tillid har til denne sektors cybersikkerhed.

Af Flemming Kjærsdam

"Ingen vej udenom NIS2 for kommunerne"

Cybertruslerne banker på hos kommunerne. IT- og digitaliseringschef Henrik Brix, Favrskov Kommune, siger, at der næppe går en dag uden, at cybertruslen vendes og drejes blandt kollegaer. Især har Europas konflikt med Rusland, skærpet opmærksomheden i kommunen. EU har netop vedtaget NIS2-direktivet som udvider kravene til cybersikkerhed. Og selvom det ikke er besluttet, at kommunerne er omfattet af NIS2-direktivet, "er der ingen vej udenom", ifølge Henrik Brix.

Efter Ruslands invasion i Ukraine i 2022, fylder IT-sikkerheden langt mere i landets kommuner. Ifølge IT-og digitaliseringschef Henrik Brix, Favrskov Kommune, er cybertruslen et emne, der tales om dagligt i kommunerne på grund af de mange forsøg på angreb.

Det har gjort, at Favrskov Kommune har sat en række tiltag i gang for at beskytte data bedre.

"Først har vi en mere omfattende sårbarhedsscanning. Hvor er de huller i vores netværk og systemer, som hackerne leder efter til at bryde ind og få adgang. Vi har også iværksat geoblocking. Det vil sige, at IP-adresser fra seks-otte lande bliver automatisk blokeret af serverne. Og vi har gennemført mere overvågning af en række it-systemer. Det, vi ikke kan vide, er, om det er nok. Det er det formentlig ikke," siger Henrik Brix.

Samme dag som interviewet havde en russisk hackergruppe væltet Finansministeriets hjemmeside og gennemført angreb mod syv banker, herunder Nationalbanken.

"Vi har også strammet op på vores interne procedurer for vores udstyr. Vi tager en retning mod "nul tillid", vi stoler ikke på nogen, og hver gang en bruger logger på, skal du identificere dig yderligere. Det er lidt mere besværligt og lidt mere bøvlet, men der er ikke andet at gøre. Det er en omkostning ved at digitalisere så meget, når truslerne vokser. Da cybertruslen flytter sig til det værre, er vi nødt til løbende at justere vores politikker på en række områder f.eks mere sikkerhed ved log-in," siger Henrik Brix.

Senest har Center for Cybersikkerhed hævet sit trusselsniveau fra middel til høj. Lampen blinker rød. Trusselsniveauet er stigende og især den russiske hacktivisme, som er en slags "politisk selvtægt", er om sig.

"Foran vores fysiske dør, står politiet og forsvaret. Foran vores firewall er der ingen vagt. Det skal vi selv sørge for. Man kan diskutere hvad en sikkerhedshændelse er. Hvis phishing, som er den mest udbredte cybertrussel med 69 pct. i PwC´s survey, er, at vi har modtaget en mail, der forsøger at få en medrbejder til at klikke på et link, så vil jeg sige, det sker hver dag og er tættere på 100 pct. Men hvis medarbejderen ikke klikker på linket, er der ingen skade sket. Så alvorligheden i angrebene er meget forskellig. DDoS er jo ikke kompromittering af data. Det er snarere en slags sabotage," siger Henrik Brix.

Phishingangreb er det mest udbredte for alle tre sektorer.

"Det er genkendeligt. Jeg noterer mig, at det offentlige har flere fejl forårsaget af leverandører. Utilsigtet deling af følsomme oplysninger er relativt stor hos offentlige brugere. Vi behandler mange følsomme oplysninger, så det er nok naturligt, at det forholder sig sådan, men det er naturligvis ikke i orden".

Flere penge til sikkerhed

NIS2-direktivet skal implementeres i dansk lov. "EU-medlemslandene har vedtaget NIS2-direktivet, der udvider kravene til cybersikkerhed og sanktionerne ved manglende overholdelse af disse for at harmonisere og strømline sikkerhedsniveauet på tværs af medlemslandene."

"Endnu er det ikke helt afklaret, om kommunerne bliver omfattet men det forventer jeg. Der er ingen vej udenom, selv om der er nok at lave uden," siger Henrik Brix.

Kommunerne kommer til at bruge flere ressourcer og penge på sikkerhed.

"Budgetterne er ikke hævet endnu. Men vi skal igang med samarbejdet med DCIS Sund, og det kommer til at koste penge. Vi kommer til at bruge flere ressourcer – men det er svært at finde pengene, da de skal tages fra noget andet. Nogle vil formentlig blive taget fra digitalisering og flyttet over til IT-sikkerhed visse steder. Jeg kan ikke se, hvorfor kommunerne ikke skal være med i NIS2. Kommunerne dækker en række samfundskritiske områder, som kommunal hjemmepleje og arbejdsmarked. Det første step er tilslutning DCIS Sund, og det skal gennemføres i samarbejde mellem alle 98 kommuner. Det har jeg ret store forventninger til," siger Henrik Brix.

I PwC´s Cybercrime Survey af 2022 falder kommunerne dårligere ud end de øvrige sektorer. Det er jo ikke kvaliteten af sikkerhedsarbejdet, der spørges ind til. Det er tilliden til til kommunernes evne til at beskytte data.

"Omkring GDPR-compliance og cybersikkerheden er det et faktum, at kommunerne behandler mange flere persondata, altså følsomme persondata, end de fleste andre sektorer." Det er jo også en af forklaringerne på, at utilsigtet deling af følsomme personoplysninger eller anden følsom information er højere, fordi andelen af følsomme data er langt højere end staten. Kommunerne er den sektor, der har kontakten med borgerne, hvor sikker behandling af følsomme oplysninger er en del af kerneydelsen. Men når det er sagt, kan det også blive bedre," siger Henrik Brix.

Kommunerne ser en mindre i fremgang i 2022 i forhold til 2021. Men ligger stadig dårligere end staten og den finansielle sektor.

Af en leverandøropgørelse fra IDC Nordic fremgår det, at finanssektoren bruger minimum fire gange så meget på eksterne leverandører end det offentlige gør.

"De flere penge, som den finansielle sektor investerer pr. medarbejder, kan også være en grund til, at folk har mere tillid til databeskyttelsen," siger Henrik Brix.

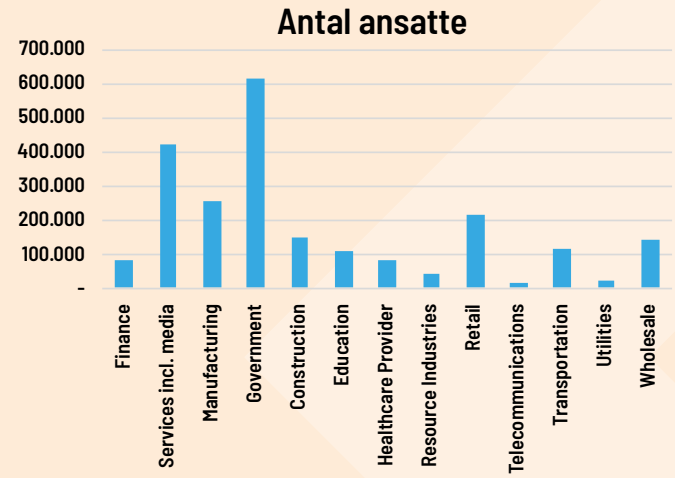
«««

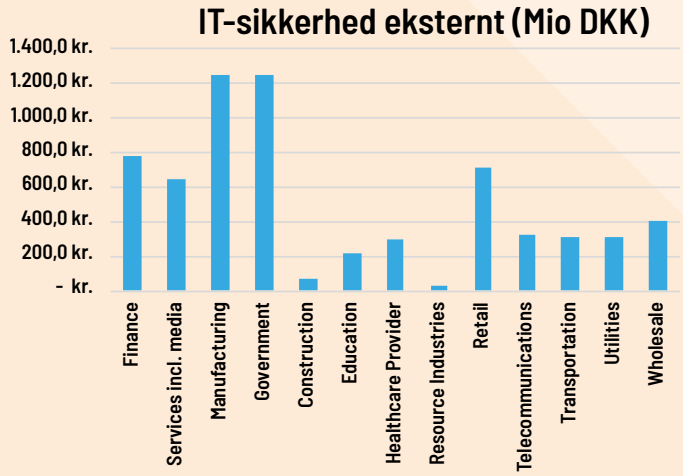
IT-sikkerhed i Danmark

IDC Nordic har opgjort investeringer i IT-sikkerhed i Danmark for 13 udvalgte sektorer.

Den øverste graf viser antallet af ansatte i de 13 sektorer. 82.039 i finanssektoren, 423.315 i services og medier, 256.827 i fremstillingsindustrien og 616.338 i det offentlige.

I den anden graf kan man se at finanssektoren bruger 780 mio. kr. på eksterne leverandører. Services og medier investerer 638,4 mio. Kr. Fremstillingssindustri investerer 1241,5 mio. Kr. og det offentlige samlet 1246,8 mio. kr.





Graferne dækker over 327.000 virksomheder der tilsammen investerer 112 mia. kr. i hardware, software, kommunikation og konsulenter. Virksomhederne beskæftiger i alt 2.266.300 ansatte

Kilde: IDC Nordic/Danmarks Statistik

KITA TEMA

Af Flemming Kjærsdam

På vej mod et nyt overførsels-grundlag med amerikanske cloudløsninger

USA og EU er ved at bilægge den konflikt, der har været med de såkaldte "tredjelandsoverførsler", som opstod i kølvandet på EU-domstolens Schrems II afgørelse den 16. Juli 2020. Her faldt overførselsgrundlaget "Privacy Shield" med et brag, og virksomheder og myndigheder var overladt til EU-Kommissionens standardkontrakter, som er meget "lidt praktiske" at anvende. Ifølge formanden for Rådet for Digital sikkerhed, Henning Mortensen, er der et nyt overførselsgrundlag på vej, som vil lovliggøre brugen af amerikanske cloudløsninger.

I november 2022 skrev USA´s præsident Joe Biden et præsidentielt dekret til EU-Kommissionens formand Ursula von der Leyen. I dekretet ændrede Joe Biden betingelserne for masseovervågning og gav desuden de europæiske borgere, der mente, at deres personfølsomme data var blevet misbrugt, en ny civilret, hvor de vil kunne rejse deres sag. Det er to helt centrale punkter, hvor Joe Biden kommer EU-domstolens afgørelse i møde.

"Vi er ikke i mål endnu. Det Europæiske Databeskyttelsesråd (EDPB) skal først høres. Men Kommissionen har nikket ja til indholdet i Bidens dekret. Derfor vurderer jeg, at vi kan være på vej mod et nyt overførselsgrundlag, selv om EDPB ikke har offentliggjort deres bemærkninger,"siger Henning Mortensen.

Baggrund

Med schrems II afgørelsen fra EU-domstolen den 16. Juli 2020, blev det hidtidige overførselsgrundlag "Privacy shield" dømt ude, da det ikke ydede borgerne tilstrækkelig sikkerhed inden for beskyttelse af persondata. Det vil sige, at alle myndigheder og virksomheder har været henvist til at bruge kommissionens standardkontrakter. EDPB har lavet den vejledning med en sekstrins model, hvor en kommune, der overfører data til lande med problematisk lovgivning, f. eks. USA, skal kryptere data og sørge for, at de aldrig er tilgængelige i klar tekst.

Henning Mortensen: "Det omfatter stort set alle dataoverførsler, vi laver til de amerikansk ejede cloud tjenester, så det er et meget stort problem, som vil gøre det vanskeligt at bruge cloudservices fremover og dokumentere, at det er compliant med GDPR-forordningen".

"For at rette op på det, og for at kunne etablere et nyt overførselsgrundlag efter artikel 45, skal EU-Kommissionen lave en tilstrækkelighedsopgørelse. Amerikanerne har justeret noget af deres lovgivning. De opstiller formål, hvor de begrænser masseovervågning og hvad man må bruge data til. Og på den baggrund mener vi, at de er ude i noget, som faktisk kan siges at være lovligt efter EU-domstolens afgørelse. Desuden etablerer de en domstol, hvor man kan få prøvet sine sager. Det var den anden ting, som EU-domstolen i 2020 sagde, var ulovligt, at den mulighed ikke eksisterede," siger Henning Mortensen.

Joe Biden imødekommer europæerne på de her to meget væsentlige punkter. Og kommissionen går ind og kigger på dekretet med den nye retstilstand og laver deres tilstrækkelighedsopgørelse.

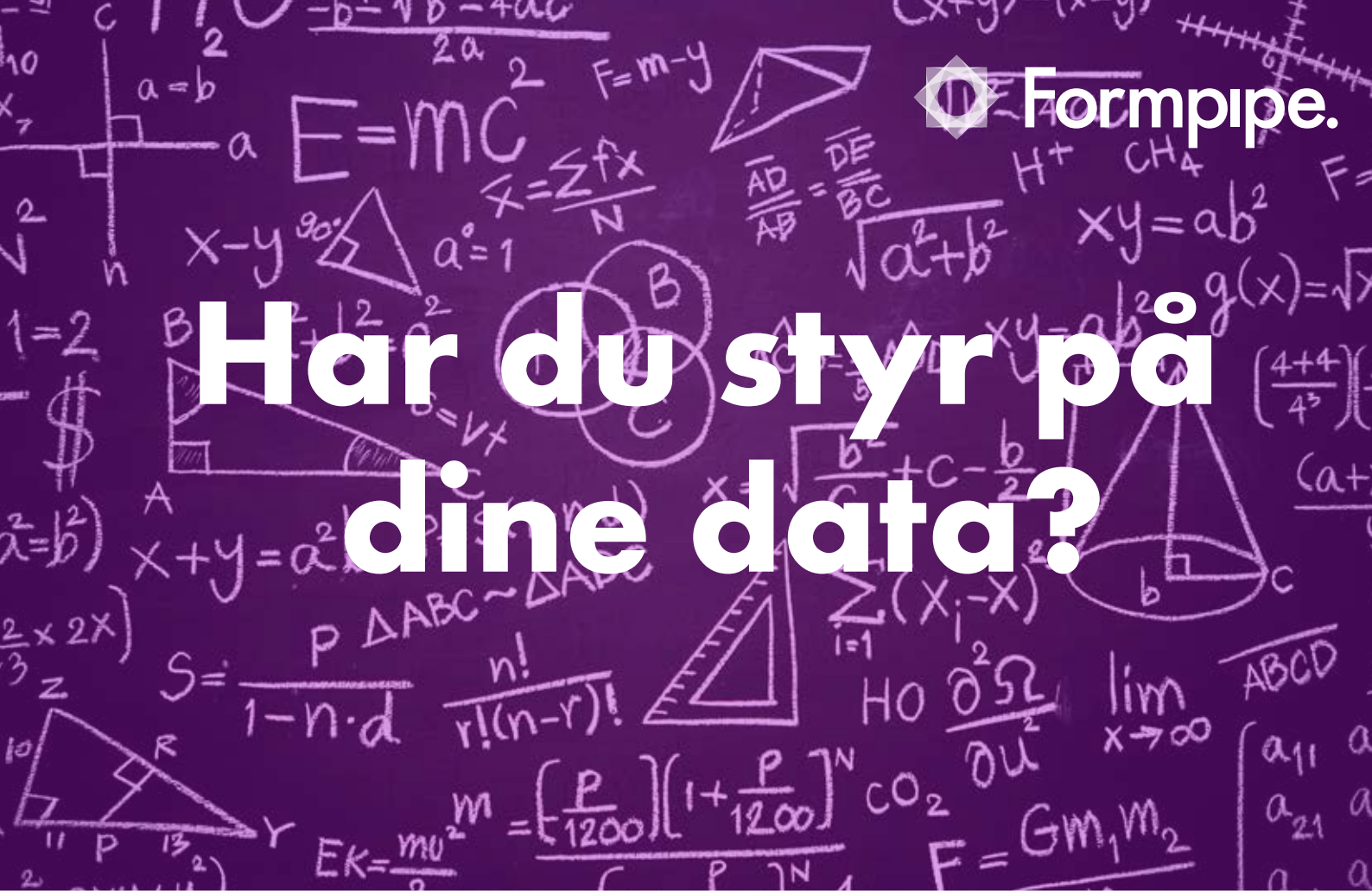
"Alt i alt vil begrænsninger på hvad masseovervågning må anvendes til, og etableringen af den nye domstol, så mener EU-Komissionen, at det er et essentielt ækvivalent beskyttelsesgrundlag i USA svarende til hvad vi har af garantier i Europa. Naturligvis under forudsætning af, at de amerikanske ejede, som man overfører data til, også efterlever de nye regler, der vil gælde som et nyt overførselsgrundlag. Amerikanerne laver nemlig mulighed for, at de kan have nogle andre krav," siger Henning Mortensen.

Max Schrems, den østrigske jurist, der har lagt navn til EU-domstolens afgørelser i 2015 og 2020, har i en pressemeddelelse i januar 2023 lagt afstand til Joe Bidens dekret. Han lægger dermed op til, hvis Joe Bidens dekret bliver rammen for et nyt overførselsgrundlag, at det skal prøves af ved domstolene en gang mere.

‹‹‹

"Vi er ikke i mål endnu. Det Europæiske Databeskyttelsesråd (EDPB) skal først høres. Men Kommissionen har nikket ja til indholdet i Bidens dekret. Derfor vurderer jeg, at vi kan være på vej mod et nyt overførselsgrundlag, selv om EDPB ikke har offentliggjort deres bemærkninger.

Bestyrelsesformand Henning Mortensen, Rådet for Digital Sikkerhed



Det skal ikke være raketvidenskab.

For hver dag, time, minut og sekund stiger datamængden hos os alle. **MEN**, glem alt om tidskrævende oprydningsdage, uoverskuelige risikoanalyser, søvnløse nætter og kontrol af medarbejdere. Sig i stedet for goddag til din nye digitale assistent, **Adoxa**, som giver dig en GDPR-compliant hverdag med 100% styr på alle personfølsomme data på tværs af dine IT-systemer.

Det skal ikke være raketvidenskab at have styr på sine data. **Adoxa** sikrer en proaktiv og professionel håndtering af data, som én gang for alle rydder op i det som jeres virksomhed har liggende. Samtidig sikrer vores GDPR-løsning, at al ny data, der kommer både ind og ud af systemet, er i høj kvalitet og overholder samtlige krav til datasikkerhed. Mere end 50 kommuner har allerede taget **Adoxa** i brug, og det skaber både tryghed og forhindrer fejl, som ellers havde være næsten uundgåelige.

Bliv klogere på, hvordan Kolding Kommune fik styr på deres data med Adoxa

72 20 81 51

Fakta om Adoxa

- Øget effektivitet, samlet overblik og større dataindsigt
- Oprydning som medarbejderansvar
- Best practice søgeregler suppleret med egne regler
- Overskuelig visning af status og fremdrift for fokusområder
- 100% kontrol over hvem, hvor, hvad og hvornår
- On premise eller som hosted løsning
- CPR-data valideret i CPR-registre, så falske positiver undgås

Adoxa
by Formpipe.

Af Digitaliseringskonsulent Christian Christensen, KL

Arbejdet med et kommunalt værn mod cyberkriminalitet er i fuld gang

Danmarks digitale sikkerhed er truet. Center for Cybersikkerhed (CFCS) vurderer i deres seneste trusselsvurdering for Danmark, at truslen for cyberspionage og cyberkriminalitet er "meget høj" og at truslen for cyberaktivisme er "høj". CFCS vurderer at truslen er vedholdende og stigende, bl.a. med baggrund i krigen i Ukraine.

Der findes ikke et mirakelmiddel mod denne situation. Sikkerhedsfolk arbejder med beskrivelsen, at der skal arbejdes med mange lag. Der er huller i hvert lag. Lægges tilstrækkeligt med lag oven på hinanden, vil lagene dække over hinandens huller. Alt efter hvor meget man investerer af arbejdskraft, teknologi og flid i hvert enkelt lag, des færre huller bliver der igennem lagene.

Arbejdet hidtil i kommunerne

I kommunerne har der igennem mange år været arbejdet med forskellige lag af sikkerhed. De tekniske lag er f.eks. firewall, segmentering af netværk, backup og brugerstyring. De procesmæssige lag er afprøvning af beredskabsplaner, genskabelse fra backups, ændringsstyring mv.
De seneste år har "papirsikkerheden" fyldt mere. Persondataforordningen har stillet krav om fortegnelse, risikovurderinger samt konsekvensanalyser hvor det er nødvendigt for at reducere for høje risici. Politikker, roller og actioncards er udformet efterhånden som modenheden er steget. Papirsikkerhed kræver en større modenhed i organisationerne, for at man kan få gevinst af de tiltag.
Ovenstående tiltag har alene internt sigte. Dvs. de er rettet imod egen organisation. Evnen til at opdage sikkerhedsbrud, igangværende eller under opsejling, ser kun indad på egne data og trafikmønstre.

Nye krav og tilgange

Drevet af regeringens øgede fokus på cybersikkerhed, har sundhedssektoren som de første tænkt kommunerne med i nationale tiltag. Sundhedssektoren er kendetegnet ved en høj grad af digitalisering med stadig mere samarbejde om behandling og pleje af patienter på tværs af myndigheder. Fælles digitale løsninger er afgørende for udviklingen af det sammenhængende sundhedsvæsen på tværs af hospitaler, praktiserende læger, bosteder og kommunale sundhedstilbud.
Samtidig er cyberkriminalitet en alvorlig trussel mod den højt digitaliserede sundhedssektor. Hver dag er der forsøg på cyberangreb mod både myndigheder, leverandører og borgere. Data i sundhedssektoren er værdifulde for kriminelle, da de kan bruges til afpresning, falske digitale identiteter og planlægning af målrettede angreb. På det kommunale sundhedsområde kan angreb på det fælles medicinkort i værste fald betyde, at borgere dør, hvis data ikke er tilgængelige eller bliver forvansket.

PwC rapport om cyberværn

I 2022 igangsatte KL et kortlægningsarbejde med PwC som udførende.

Den første væsentlige beslutning der skal træffes er, om der er politisk opbakning til at arbejde videre med at etablere et kommunalt samarbejde på området, der principielt omfatter alle 98 kommuner.

Digitaliseringskonsulent Christian Christensen, KL

Arbejdsgruppen havde flere møder, hvor alle kommuner var inviteret med, samt en referencegruppe bestående af 26 kommuner. PwC har nu leveret en rapport, der kommer med en række anbefalinger.
Rapportens hovedkonklusioner er, at:
1. Der er et stort behov for og ønske om, at kommunerne går sammen i et forpligtende samarbejde om at løfte cyberopgaven og styrke cyberværnet af alle de kommunale aktiviteter. Dels for at sikre et tilstrækkeligt fagligt niveau. Dels for at sikre en effektiv anvendelse af de samlede kommunale ressourcer og kompetencer.
2. PwC anbefaler fem trin for etablering af et fælleskommunalt cyberværn. De 5 trin er:
a. Kommunal tilslutning til DCIS Sund, der giver adgang til tværgående viden fra "Opdage services" på sundhedsområdet.
b. Etablering af organisation til fælleskommunalt cyberværn og kommunal tilslutning til dette, herunder adgang til grundlæggende fælles kapaciteter med relevante kompetencer.
c. Fælleskommunalt cyberværn udbyder og implementerer "Opdage services" for de tilsluttede kommuner. Alle kommunens områder er med her.
d. Kommunerne kan tilslutte sig "Reagere" og eventuelt "Gendanne" services via fælleskommunalt Cyberværn.
e. Kommunerne kan tilslutte sig yderligere services via fælleskommunalt cyberværn.

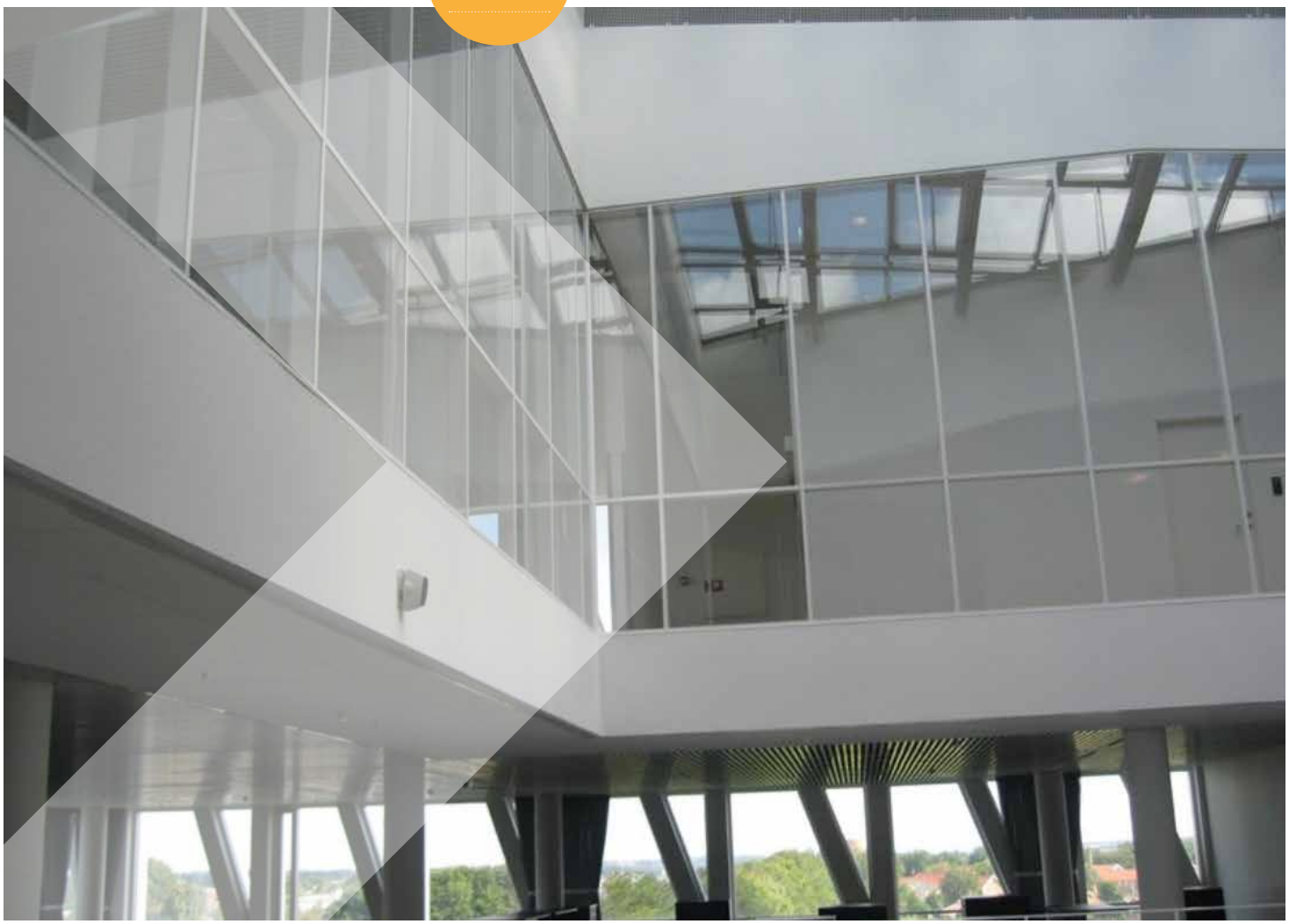
Cyberværn i flere ord

PwC rapporten peger på en række områder, hvor kommunerne med fordel kan styrke samarbejdet. Kompetencer inden for cyber- og informationssikkerhed er en mangelvare på det danske arbejdsmarked. At etablere en organisation med stærke kompetencer, der kan samle og facilitere udviklingen for kommunerne, vil derfor styrke både viden og udnyttelse af de eksisterende ressourcer (trin b).
At opdage, forebygge og reagere på cyberkriminalitet på tværs af landets kommuner, og øvrige offentlige aktører kræver, at der benyttes ny teknologi. Med udgangspunkt i DCIS Sunds viden om "NDR "-teknologien, påpeger rapporten en fordel i at bygge videre på det (trin a). Kort fortalt kan NDR-teknologien opbygge billeder af en normal trafik på indersiden af hver kommunes firewall. Afvigelser fra normalsituationen rapporteres til en central analyseenhed (trin c), der herefter kan afgøre hvad der vil være passende at gøre. Disse trin skal omfatte alle kommunernes arbejdsområder, ikke kun sundhedsområdet.
Anbefalingen er, at der til en start styrkes muligheden for at opdage mere og tidligere end i dag, men hvor de tilkoblede kommuner primært skal reagere lokalt. Med tiden kan der så udbygges yderligere med egentlige incident response teams (trin d), der kan hjælpe med at gendanne og reagere på angreb.

Hvordan kommer vi til at bruge PWCs analyse og anbefalinger?

Den endelige plan for 2023 og frem er ikke lagt endnu, da der fortsat er nogle elementer der skal fastlægges. Og de forskellige veje skal drøftes. Den første væsentlige beslutning der skal træffes er, om der er politisk opbakning til at arbejde videre med at etablere et kommunalt samarbejde på området, der principielt omfatter alle 98 kommuner. Hertil skal den gode organisering for samarbejdet findes. Det kan være en forening som det Fælleskommunale Databehandler Sekretariat, det kan være KOMBIT der varetager opgaven, men der kan også være andre modeller.
I KL er vi i gang med at afklare den politiske opbakning til at arbejde videre med et kommunalt cyberværn. Når dette er afklaret og såfremt der er opbakning, vil der skulle arbejde med at finde ambitionsniveauet for samarbejdet. Skal der startes med de tre første trin (a – c) i PWC's rapport, eller skal vi gå hele vejen med det samme? Hvad er økonomien bag hvert trin? Og hvordan finansieres det?
Hvis det besluttes at arbejde videre med et fælleskommunalt samarbejde på cyber- og informationssikkerhedsområdet, skal det også afklares hvordan der sikres kompetencer til samarbejdet, juridiske aspekter omkring datadeling, tilslutningsaftaler, driftsaftaler mv. Herunder om en del af disse opgaver skal afløftes med udbud.

Af Flemming Kjærsdam



Databehandlersekretariatet i Viborg er kommet flot fra land

Databehandlersekretariatet (DBS) i Viborg er kommet flot fra land. Kontoret blev åbnet i august 2022 og skal føre tilsyn med databehandleraftalerne, som kommunerne indgår med leverandørerne.

"Det er en fornøjelse, at kommunerne synes, det giver værdi. Det næste er, at de leverandører, vi støder ind i, ligeledes giver udtryk for, at det også skaber værdi for dem," siger bestyrelsesformand Erik Sørensen, DBS, som er tidligere IT- og digitaliseringschef i Viborg Kommune.

Da DBS blev etableret som forening i 2022, var der 61 kommuner, som meldte sig ind. Nu er der 63 medlemmer. Senest har Struer og Langelands kommuner meldt sig under fanerne i DBS. Sekretariatet har nu fem ansatte.

Sekretariatschef Henrik Houmøller Sprøgel, DBS: "Vi har oplevet stor interesse fra en række kommuner. Først og fremmest fra medlemmerne, men vi oplever også interesse fra kommuner, der ikke har meldt sig ind fra starten af. Det positive er, at sekretariatet allerede nu er nået langt."

De første tre måneder fra august til og med oktober 2022 er gået med etableringen af sekretariatet. At ansætte medarbejdere, at opbygge systemer og få faktureret kommuner, så Sekretariatet kan fungere. I november, december og januar er de 30 første tilsynsrapporter blevet udarbejdet og publiceret til de 62 kommuner.

"Det er en meget spændende opgave, sekretariatet er sat til at løse på kommunernes vegne. Jeg sad i en driftsopgave i en kommune, og erfarede at tilsynet med databehandleraftaler, som er en konsekvens af GDPR-forordningen fra EU, kommer skævt ind i en driftsopgave. Derfor giver det god mening at pille databehandleraftalerne ud og løse dem fælleskommunalt i DBS. Det skaber både værdi for kommuner og leverandører. Kommunerne sparer tid til administration og leverandørerne kan få deres databehandleraftaler godkendt et sted for mange kommuner, så de undgår mange forskellige versioner af deres databehandleraftaler og at bruge tid på vedligeholdelsen af dem," siger Henrik Sprøgel.

Databehandleraftalerne

EU's Databeskyttelsesforordning med GDPR-reglerne har skærpet kravene til kommunernes behandling og kontrol af personoplysninger. Kommunerne skal som dataansvarlige kunne dokumentere, at de kontrollerer de leverandører, som leverer it-systemer til kommunerne, om de opfylder GDPR-reglerne i behandlingen af borgernes data. Der er både tale om beskrivelser af it-systemer og databehandleraftaler og risikovurderinger. Det er den samlede mængde af det arbejde, der er lagt ind i Databehandlersekretariatet.

Sekretariatet skal tage udgangspunkt i de systemer, som mindst 20 kommuner bruger. "Der ligger 370 databehandleraftaler i den pulje. Det er oceaner af timer, der bliver sparet i kommunerne, ved at sekretariatet gør det," siger Erik Sørensen.

Selvom det Fælleskommunale Databehandlersekretariat løser opgaven om databehandleraftaler, kan kommunerne ikke fraskrive sig ansvaret for aftalerne. Populært sagt kan kommunerne ikke fraskrive sig ansvaret ved at outsource tilsynsopgaven.

Kommunerne skal underskrive databehandleraftaler for hvert eneste system og hver eneste leverandør og kontrollere om leverandørerne behandler persondata efter GDPR-reglerne.

"Formålet med etableringen af Databehandlersekretariatet er, at kommunerne fremover vil gøre arbejdet i fællesskab i stedet for at gøre det hver for sig. Vi skal som dataansvarlige kigge ned i den enkelte databehandleraftale og i revisionens bemærkninger. Du bliver som dataansvarlig nødt til at være nede i databehandlingen i de systemer vi bruger. Du skal ligeledes være opmærksom på underdatabehandlere på listen. Når vi så får listerne, er der nogle af dataoverførslerne, der er landet i tredjelande uden for EU," siger Erik Sørensen.

- fortsættes på side 30 »»»

"Derfor giver det god mening at pille databehandleraftalerne ud og løse dem fælleskommunalt i DBS. Det skaber både værdi for kommuner og leverandører. Kommunerne sparer tid til administration og leverandørerne kan få deres databehandleraftaler godkendt et sted for mange kommuner.

Sekretariatschef Henrik Houmøller Sprøgel, DBS

SÆT X I KALENDEREN

KOMMENDE ARRANGEMENTER I KITA 2023

KITA Generalforsamling og Temadag

Den 2. og 3. marts 2023 på
Hotel Koldingfjord.
Tema: Cybersikkerhed.
Tilmeldingsfrist den 25. februar.
Se program og tilmeld dig på www.itchefer.dk

Netværksmøde i KITA Informationssikkerhedsnetværk

Den 30/3 hos Severin Kursuscenter i Middelfart.
Deltagelse er gratis (no-show gebyr på kr. 500,- + moms).
Se programmet og tilmeld dig i netværksgruppen på www.itchefer.dk
Tema: NIS2 og awareness.

KITA Efterårsseminar

Den 14. og 15. september 2023 på Hotel Koldingfjord.
Nærmere information følger.

Digitaliseringsmessen23

Den 27. september 2023 i Odense Congress Center.
Nærmere information følger.

itchefer.dk

KITA
Kommunale IT- og Digitaliseringsansvarlige

Det nye sekretariat hedder Det fælleskommunale Databehandlersekretariat (DBS).

- **Bestyrelsen for foreningen består af otte medlemmer. Erik Sørensen, Viborg Kommune, er formand for bestyrelsen.**
- **Sekretariatet skal føre tilsyn med de databehandleraftaler, som mere end 20 af foreningens medlemmer har indgået med leverandører og øvrige samarbejdspartnere.**
- **Sekretariatet kan også forhandle databehandleraftaler og lave risikovurderinger af de databehandlinger, som aftalerne omfatter.**

FAKTA

Kontingent i 2023

Kategori 1 – 0-50.000 indbyggere	100.000 kr.
Kategori 2 – 50.000-100.000 indbyggere	130.000 kr.
Kategori 3 – 100.000-200.000 indbyggere	160.000 kr.
Kategori 4 – over 200.000 indbyggere	200.000 kr.

To opgaver

Opgaverne i DBS deler sig i to. Første del er produktionen af tilsynsrapporter, hvor DBS har lagt navn til foreløbigt 30. Det er Henrik Houmøller Sprøgel ganske godt tilfreds med. Den anden del omfatter forhandlinger med leverandørerne om indgåelse af databehandleraftaler for medlemmerne af DBS. Den opgave er DBS ikke rigtigt kommet i gang med endnu. Men den kommer til at fylde meget i indeværende år.

"Den anden opgave er at forhandle og indgå databehandleraftaler med leverandører på vegne af medlemmerne. Vi kigger ind i en portefølje af 400 it-systemer, som kommunerne hver for sig har indgået databehandleraftaler med. Vores opgave bliver at lave et gennemsyn og kontrollere, at de lever op til reglerne. Den opgave løser vi på vegne af de 63 kommuner, så de ikke selv sidder med den."

"Men forhandlingerne med leverandørerne kan også omfatte helt nye it-systemer, så vi kan lave en fælleskommunal databehandleraftaler f.eks. for et journalsystem eller sagsbehandling Vi kan også lave fælles aftaler for it-systemer der allerede er taget i drift, men hvor der sker noget nyt. Det kan være en opgradering eller ændringer, så kan vi komme ind i billedet," siger Henrik Houmøller Sprøgel.

Leverandørerne

DBS mødes jævnligt med nogle leverandører. Her er der, ifølge DBS, stor interesse for at samarbejde med DBS. DBS deltog før jul i et møde med KL, hvor der deltog en række leverandører, som gav udtryk for, at de gerne vil samarbejde med DBS.

Erik Sørensen: "Leverandørerne viser stor interesse for at samarbejde med os. Det kom frem på mødet, men også i de opfølgende snakke vi har haft med leverandører. Det er en klar fordel for leverandørerne at løse opgaver om databehandleraftaler i et centraliseret forum frem for at gøre det enkeltvist med kommunerne. Det er nemmere at tale med et sekretariat, der repræsenterer 63 kommuner, så skal de kun tage hen et sted. Det er klart det sparer tid. Og sparet tid er som bekendt penge for alle parter".

"Leverandørerne viser stor interesse for at samarbejde med os.

Bestyrelsesformand Erik Sørensen, Vibork Kommune

FIBERALLIANCEN

Fibernet er Danmarks mest udbredte digitale infrastruktur

I hovedparten af de 98 kommuner er dækningen med fibernet over 80%.

Vi er kommet langt, men vi er ikke i mål.

Mere end 1 million husstande skal tilsluttes fibernettet de kommende år.

I den forbindelse har vi en klar opfordring til alle kommuner:

1. Gør det muligt for graveaktører at efteranmelde mindre gravearbejder – såsom eftertilslutninger. Det vil gøre det lettere og hurtigere for borgerne at få fibernet.

2. Vær med til at understøtte den lokale udvikling af den digitale infrastruktur. Støt aktivt op om borgerinitiativer, som fremmer dækning med fibernet i underforsynede områder i kommunen.

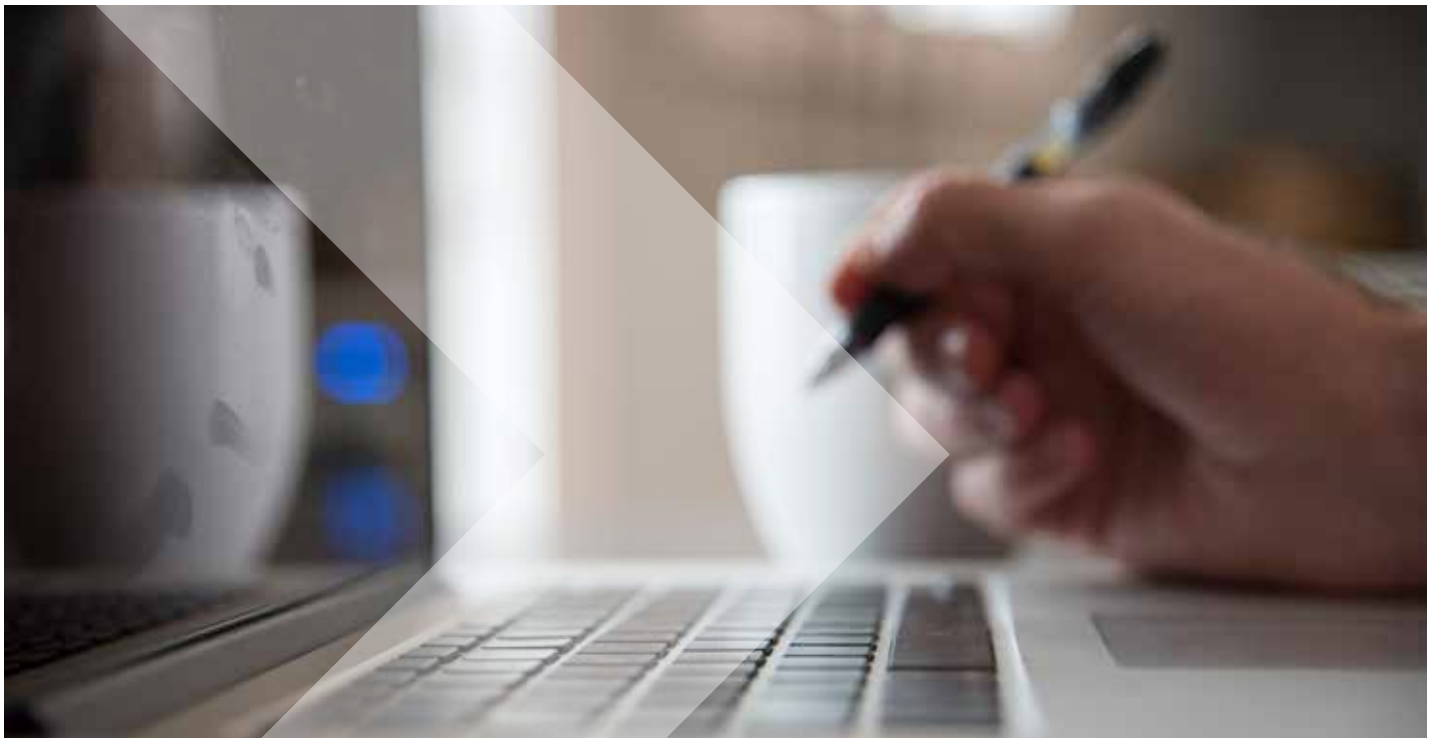
3. Brug fibernettet til at skabe bedre og mere effektiv service til borgere og virksomheder gennem digitale tilbud med højere kvalitet end ved brug af gammel digital infrastruktur.

Om Fiberalliancen Fiberalliancen er Danmarks største branchefællesskab for fibernet og samler alle de danske energi- og fibernetkoncerner, som i snart to årtier har været hovedaktørerne i udbredelse af fibernettet. Fiberalliancen er en del af Green Power Denmark, Danmarks grønne erhvervsorganisation. **Læs mere på fiberalliancen.dk**

Af Flemming Kjærsdam

Dragør Kommune er NSIS godkendt

Dragør Kommune har fået underskrevet sin revisionserklæring om NSIS (National Standard for Identitets Sikring) hos BDO Revision. Revisorgodkendelsen er sendt videre til Digitaliseringsstyrelsen, som giver den endelige godkendelse.



Dragør Kommune har ifølge it-chef Jan Jansen brugt 800 timer på at opnå revisorfirmaets underskrift af NSIS. Først fik Dragør Kommune en pre-audit den 21. september 2021 og siden kom så den rigtige audit den 23. august 2022. Både ved pre-audit og audit havde revisorfirmaet en række rettelsespunkter til kommunen. Så det har været en kæmpe opgave at implementere for it-afdelingen, da arbejdet med NSIS er kommet oveni de øvrige it-opgaver.

Dragør Kommune er sammen med Albertslund Kommune medlemmer af Den storkøbenhavnske Digitaliseringsforening (DSD) og de er udpeget som testkommuner. DSD består af 11 kommuner og Dragør har valgt løsningen fra Signaturgruppen, mens Albertslund har valgt en løsning fra OS2-fællesskabet.

"Vi har brugt mindst 800 timer i it-afdelingen for at opnå NSIS-godkendelse. Jeg klager ikke for opgaven skal løses. Men det havde været rart, om det, der bliver efterspurgt, havde ligget i et kravbilag. Langt det meste af tiden er gået med diskussioner om fortolkninger af de spørgsmål, der stilles i bilagene. Sådan har det været lige fra starten. Jeg skyder ikke på revisionsfirmaet, men snarere på Digitaliseringsstyrelsen som kunne have leveret et skema eller en skabelon med de krav, som kommunerne skal opfylde. Nu skal vi udfylde skemaer med egne fortolkninger, som revisorfirmaet skal godkende," siger Jan Jansen.

Central betydning for identitetssikring

NSIS har central betydning for identitetsløsninger som MitID og MitID Erhverv/NemLog-in samt en række decentrale fagsystemer, som kommunale it-organisationer med en Lokal IdP benytter. Lokal IdP hed tidligere medarbejdersignatur i NemID.

Ibrugtagningen af NSIS vil derfor medføre en række krav til de parter, der ønsker at blive tilkoblet den nationale digitale infrastruktur, herunder tjenesteudbydere, brugerorganisationer og brokere. Kravene i NSIS er rettet mod de betroede kommunale medarbejdere, som bruger deres identiteter over for andre, mens modtagere af identiteter ikke er underlagt kravene i NSIS, men alene skal forholde sig til det sikringsniveau, som brugeren tilgår deres tjeneste med.

En stor del af NSIS omfatter ISO 27001 compliance – den internationale standard for informationssikkerhed. Det er ikke nok, at kommunen kun har sine egne nedskrevne regler. Revisionserklæringen omfatter også, at kommunen skal dokumentere, at den overholder "principperne i ISO27001". Det er i virkeligheden her det store skifte er.

Digitaliseringsstyrelsen kræver, at der er en godkendt opkobling mellem det lokale IdP, der overholder NSIS-standarden, som via NemLog-In3 sikrer opkoblingen til de fællesoffentlige systemer. Det skal være på plads for at få en revisionserklæring.

Pre-audit tog 500 timer

Da Dragør Kommune fik sin pre-audit efter 500 timers indsats, tænkte it-chefen, at nu var kommunen omtrent i mål. Men nej. Der blev efterspurgt yderligere materialer i form af 17 overpunkter med tilknyttede underpunkter. Efter 300 timers yderligere arbejde frem mod den endelige audit, kom der så 45 rettelser ved selve audit. Det har været en lang og sej kamp for at nå frem til målet.

Digitaliseringskonsulent Jens Erik Rolighed Larsen, Dragør Kommune: "Som jeg husker det, havde jeg en meget god fornemmelse ved pre-audit efter de første 500 timer. Der var selvfølgelig nogle bump på vejen og faldgruber, men vi kom nogenlunde positivt ud af det. Vi var mere eller mindre klar til den endelige revisorerklæring. Det gik dog helt anderledes, for da vi kom til den endelige audit, var der 45 rettelser oveni. Da fandt jeg ud af at vi skulle lægge mange flere timer i det – omkring 300 timer".

De revisorerklæringer som revisorfirmaet skal underskrive har en omfattende kvalitetskontrol. I dette NSIS paradigme – år 1- er der en ekstra konsulentindsats fra revisionsfirmaets side. I og med mange kommuner vælger at tage en pre-audit først, som en slags opvarmning til en audit. At tage en pre-audit betyder, at kommunen bliver sporet ind på det arbejde, der ligger i at kunne kontrollere og dokumentere arbejdet med identitetsgodkendelse af medarbejdere samt løbende risikovurderinger.

Jan Jansen: "Vi har selvfølgelig draget vores erfaringer i forløbet vedrørende de spørgsmål, som er stillet i kravbilagene. Og jeg vil da også sige, at vi tror, at BDO også har fået erfaringer vedrørende de fortolkninger af spørgsmålene som er blevet stillet til os. Derfor er jeg godt tilfreds med, at vi valgte at være testkommune, fordi det har gjort, at vi er kommet på omgangshøjde med NSIS tidligere, end hvis vi havde været afventende. Men jeg vil også sige, at der i løbet af perioden er sket et skifte af de fortolkninger i perioden både hos os og revisorfirmaet. Så jeg vil anbefale andre kommuner om at komme i gang, hvis de ikke allerede er det".

"Som jeg husker det, havde jeg en meget god fornemmelse ved pre-audit efter de første 500 timer. Der var selvfølgelig nogle bump på vejen og faldgruber, men vi kom nogenlunde positivt ud af det. Vi var mere eller mindre klar til den endelige revisorerklæring. Det gik dog helt anderledes, for da vi kom til den endelige audit, var der 45 rettelser oveni. Da fandt jeg ud af at vi skulle lægge mange flere timer i det – omkring 300 timer.

Jens Erik Rolighed Larsen, Dragør Kommune.

"Jeg efterlyser mere klare krav fra Digitaliseringsstyrelsen om, hvad det er for en opgave revisorerne skal løse i kommunerne. Jeg synes, det er for meget op til det eksterne revisionsfirma om at definere, hvad vi skal aflevere, før vi kan få den nødvendige revisionserklæring.

IT-chef Jan Jansen, Dragør Kommune

En anden fordel ved at være testkommune er, ifølge Jan Jansen, at han er blevet kontaktet af kollegaer fra andre kommuner. På den måde har der være en række dialoger med kommuner, som har ført til at der blevet en mere fælles forståelse af de udfordringer ved at blive NSIS godkendt.

Ekstra rettelser

Et af de skifte i fortolkninger, som Dragør Kommune oplevede, var, at revisionsfirmaet langt inde i forløbet efterspurgte en hændelseslog. Altså en log over de hændelser, der havde været på systemer, som medarbejdere har brugt i forbindelse med opkobling på fællesoffentlige it-løsninger.

Jens Erik Rolighed Larsen: "Hændelsesloggen lå ikke i bilagene fra starten. Så det indgik slet ikke i pre-audit fasen. F.eks. at man skulle kunne se, om der var ting, der var blevet slettet i løbet af en sag. Det blev først efterspurgt af revisionsfirmaet allersidst i forløbet. Mange af de 45 rettelser, som kom ved audit gik på, hvordan Signaturgruppens løsning hang sammen med henblik på denne log. Og det var ikke nævnt tidligere. Her vil jeg gerne rose Signaturgruppen for, at de påtog sig denne arbejdsopgave og nu er endt med at komme med en løsning, der virker på tværs af alle kommuner. Det vil jo også betyde, at de kommuner, der bruger den løsning, vil aflevere efter de samme krav til årsberetningerne".

Ifølge Jan Jansen har Nets rettet henvendelse til Dragør og spurgt om kommunen vil være pilotkommune for NSIS. Iøvrigt sammen med Viborg Kommune.

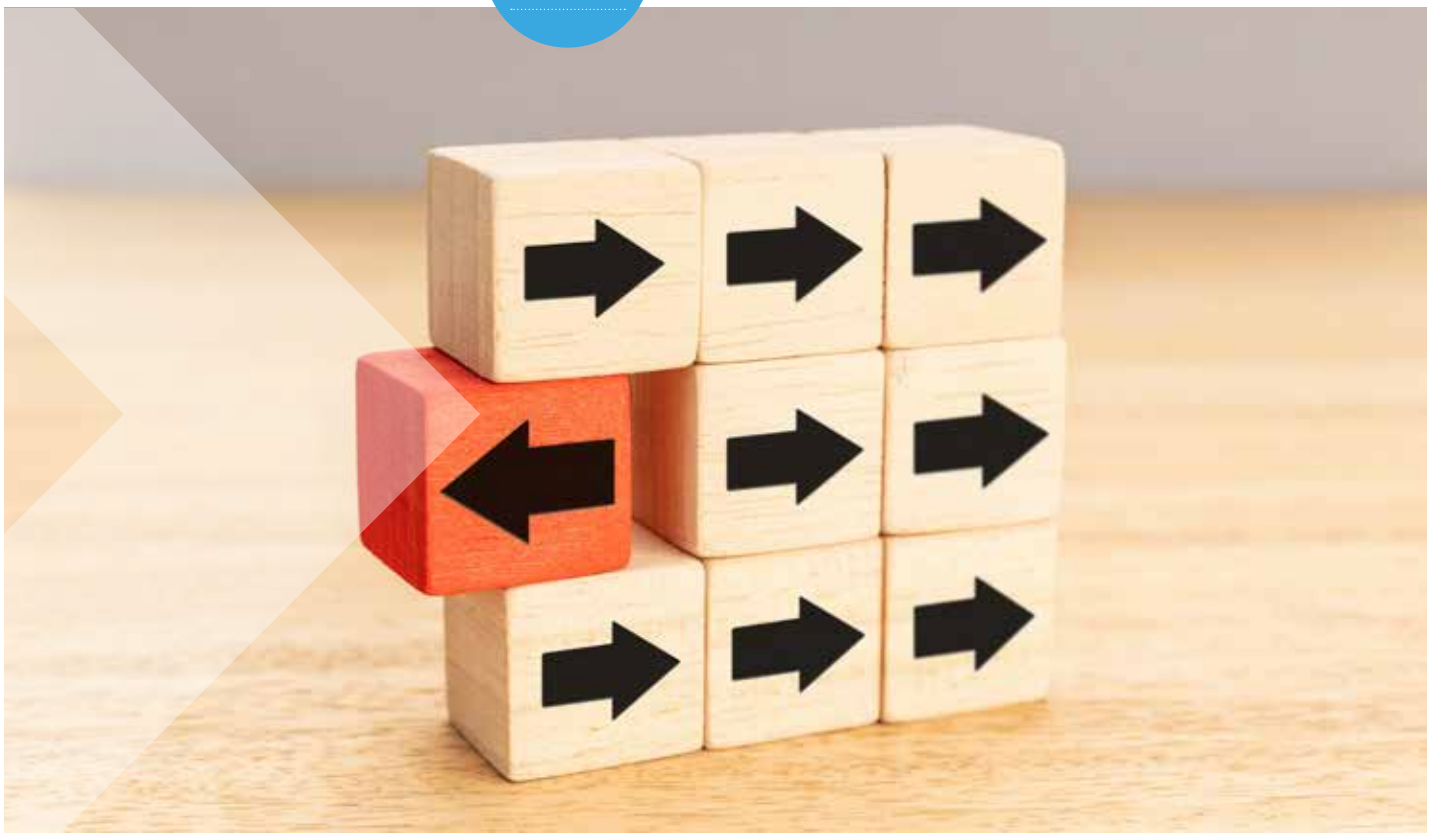
«««

FAKTA

DSD

Der er fem kommuner der benytter Signaturgruppens løsning: Høje Taastrup, Hvidovre, Dragør, Ishøj, og Brøndby. Digital Identity, som er med i OS2-Fællesskabet: Albertslund, Vallensbæk, Herlev, Solrød, Glostrup, og Rødovre.

Af Flemming Kjærsdam



Nikolaj Kolte, Holstebro:

"NSIS er godt for digitaliseringen, men uheldigt at revisionen er tildelt så meget magt"

IT- og digitaliseringschef Nikolaj Kolte, Holstebro Kommune, mener, at implementeringen af NSIS (National Standard for Identitets Sikring) er godt for digitaliseringen i landets kommuner, da det løfter sikkerheden. Men han kalder det direkte "uheldigt", at der er inkluderet ekstern revision, som hvert år skal godkende kommunens NSIS-implementering gennem en årlig certificering.

Det er noget af en opgave landets kommuner er kastet ud i med implementeringen af NSIS, som er en sikring af den enkelte medarbejders identitet, når han eller hun kobler sig på en fællesoffentlig løsning, som Skat, Virk.dk, arbejdsmarkedssystemer, sociale systemer og økonomisystemer. IT- og digitaliseringschef Nikolaj Kolte, Holstebro Kommune, mener, at NSIS er godt for digitaliseringen og sikkerheden.

"Vi får løftet vores sikkerhed, så vi fremover er sikre på, at vores medarbejdere, der logger på de nationale løsninger, også er dem, de siger, de er. Det er rigtig, rigtig godt. Det giver stor sikkerhed og autenticitet. Men jeg havde gerne set, at implementeringen af NSIS var blevet en del af den almindelige IT-revision. Nu kommer der et nyt eksternt NSIS-revisionsspor i organisationen, som kræver en årlig certificering I den proces, som vi har været igennem indtil nu, er det vores opfattelse at mange fortolkninger bliver overladt til revisoren. De har fået ret stor magt. Det havde været bedre for os, hvis Digitaliseringsstyrelsen havde stillet kravene direkte til kommunerne og en myndighed kontrollerede," siger Nikolaj Kolte.

Holstebro Kommune har i mange år benyttet sig af Signaturgruppens løsning til login. Medarbejderne kobler sig på fællesoffentlige løsninger med brugernavn en signatur og deres almindelige kodeord, som også bruges til kommunens it-systemer. Det vil kommunen også gerne have, at de kan gøre via en lokal IdP (Identity Provider) som indgang, når de

- fortsættes på side 36 »»»

Ses vi i Odense?

OffDig 23

Danmarks største konference
om offentlig digitalisering

Odeon, Odense
8.- 9. marts 2023

offdig.dk

dansk•it

skal på et fællesoffentligt system. Herefter kan medarbejderen identificere sig med MitID Erhverv og en to-faktor-enhed, som f.eks. en app eller en elektronisk nøgleviser.
"Vi har ikke brugt to-faktor login før, men vi har gennem vores nuværende løsning haft den ekstra sikkerhed lagt ind, som en integreret del af vores infrastruktur, at når brugerne for eksempel møder Virk.dk, bliver de mødt af en login prompt, hvor de skal bruge deres signaturfil, brugerid og kodeord. Så skal medarbejderne ikke huske en masse forskellige kodeord eller signaturer, hver gang de møder en ny løsning. Vi har altid taget det ret alvorligt," siger Nikolaj Kolte.
NSIS implementeringen bliver en ekstra sikkerhed, fordi privat MitID kommer med i ligningen, når den ansatte første gang ibrugtager sit MitID-Erhverv.

Temmelig længe undervejs

Ifølge projektleder, Stine Wagner Larsen, som har ansvaret for implementering af NSIS og MitID Erhverv i Holstebro Kommune, har NSIS-projektet været temmelig længe undervejs. Projektet begyndte før coronanedlukningen i begyndelsen af 2020, men under corona pandemien stod det stille - bl.a. pga. udsættelser fra Digitaliseringsstyrelsen.
"Det er den proces, vi har forberedt os på og nu er klar til. Vi besluttede ret tidligt i processen, at vi ville have en lokal IdP-løsning installeret. Fordi vi netop gerne vil fortsætte den brugeroplevelse, hvor medarbejderen kan beholde sit brugernavn og kodeord fra dagligdagen, og så derfra steppe op til NSIS. Den beslutning traf vi i 2020".
"Vi har så valgt at fortsætte samarbejdet med Signaturgruppen og implementere deres lokale IdP, for at kunne løfte brugerne over i det nye miljø på en god og sikker måde, samtidig med at vi bevarer den gode brugeroplevelse, som vi hele tiden har haft. Vi har jo sat os ind i NSIS-standarden, og brugt meget tid på at vælge det bedste tekniske set-up i samråd med Signaturgruppen. Jeg vil også sige, at det er et ret dynamisk miljø, da NSIS fortolkningerne flytter sig hele tiden, så løsningen og organisationen er også nødt til at flytte sig, fordi vi skal opfylde kvalitetskontrollerne for at få vores revisionserklæring," siger Stine Wagner Larsen.

Utryghed

At vilkårene flytter sig hele tiden skaber en vis utryghed i organisationen. Nikolaj Kolte: "Der er mange fortolkningsspørgsmål, som vi kan være nervøse for nu og her, og som vi nu skal i gang med. Vi har forberedt os godt, og vi har været alle vores processer igennem med tættekam. Vi kan sige, Vi er kommet igennem mange IT-revisioner med få anmærkninger, men med NSIS er der tale om langt flere krav med mulighed for flere fortolkninger, der rykker sig. At vi er kommet godt igennem den finansielle IT-revision betyder ikke, at det automatisk vil ske med NSIS-revisionens pre-audit. Vi har forberedt os så godt vi kan, men de fortolkningsmæssige krav og revisionens indflydelse på kravene, skaber en utryghed i organisationen."
IT-og digitaliseringschefen siger, at NSIS-opgaven har været en et besynderligt forløb med mange forsinkelser, og de strammere krav medvirker til, at ledelsen har involveret sig meget i opgaven. Holstebro Kommune arbejder efter en pre-audit i slutningen af marts 2023, og har sat en måned yderligere af til den endelige audit.
"Jeg synes, at revisionen af NSIS er en betragtelig økonomisk udgift, som vi skal sætte penge af til. Ikke nok med det, så får revisorerne en voldsom magt i audit. Vi kunne godt have tænkt os, at få nogle mere firkantede, ikke-fortolkbare krav, fra Digitaliseringsstyrelsen," siger Nikolaj Kolte.

Løfter kvaliteten

Selvom NSIS implementeringen er lang og sej, arbejder Holstebro Kommune efter at få sidegevinster ud af forløbet. De mange og høje kvalitetskontroller i NSIS, vil Nikolaj Kolte gerne have effekt af parallelt med implementeringen af identitetssikringen.
"Vi har en række ændringsprocesser (change management) om, hvordan vi opdaterer vores it-løsninger. Kan vi blive bedre til at opdatere kritiske komponenter over en bredere kam? Vi synes, vi gør det godt allerede, men NSIS implementeringen har presset os yderligere, da vi ved, vi skal revideres. Det vil vi bruge til at forberede opdateringer af software i vores infrastruktur på vores netværk endnu bedre," siger Nikolaj Kolte.
Nikolaj Kolte fortæller videre, at der tidligt i processen blev implementeret nye brugerrettede værktøjer, som kræves for at ibrugtage i NSIS i praksis. F.eks. egenkontrol af kodeord. "De processer har vi indført, så medarbejderne skal autentificeres via privat MitID. Nu kan en medarbejder ikke bare ringe ind til vores servicecenter, og få skiftet sit kodeord. Så dele af de værktøjer, som skal bruges af medarbejderne, når vi begynder at anvende NSIS lokal IdP'en, er allerede implementeret. Næste skridt bliver to-faktor login for step-op til NSIS, når det kræves af it-systemet."

Det er den proces, vi har forberedt os på og nu er klar til. Vi besluttede ret tidligt i processen, at vi ville have en lokal IdP-løsning installeret. Fordi vi netop gerne vil fortsætte den brugeroplevelse, hvor medarbejderen kan beholde sit brugernavn og kodeord fra dagligdagen, og så derfra steppe op til NSIS. Den beslutning traf vi i 2020.

Projektleder NSIS/MitID Erhverv Stine Wagner Larsen, Holstebro

Det er vores opfattelse at mange fortolkninger bliver overladt til revisoren. De har fået ret stor magt. Det havde været bedre for os, hvis Digitaliseringsstyrelsen havde stillet kravene direkte til kommunerne og en myndighed kontrollerede

IT- og digitaliseringschef Nikolaj Kolte, Holstebro.

Ingen generel deadline for NSIS-revisions-erklæring

Digitaliseringsstyrelsen oplyser, at der ikke er sat en generel frist for, hvornår kommunerne skal have indsendt en revisionserklæring for få godkendt NSIS-standarden. NSIS er (National Standard for Identitets Sikring). Når en kommunal medarbejder logger sig på en fællesoffentlig løsning fra en kommunal digital enhed skal medarbejderen autentificeres via NSIS standarden.

"Myndighedstilsynet stiller ingen krav til kommuner eller andre aktører om, hvornår eller hvorfor kommuner eller organisationer herunder skal være NSIS godkendt," skriver Digitaliseringsstyrelsen.
Men der kan indirekte komme deadlines via krav om sikringsniveau fra tjenesteudbydere som Aula, SkoleIntra, Meebook, eller fra brokere, som kommunerne benytter sig af i forbindelse med en arbejdsproces for identifikation, autentifikation og autorisation af kommunernes medarbejdere og/eller slut-brugere.
Et eksempel kan læses på hjælpesiden "Lokal Idp – frist for anmeldelse" under Styrelsen for IT og Læring STIL i Børne og Undervisningsministeriet, hvor det hedder, at: "Hvis en lokal IdP ikke er NSIS- anmeldt, og derfor ikke fremgår af Digitaliseringsstyrelsens oversigt over NSIS-anmeldelser pr. d. 1. marts 2023, vil det medføre, at den lokale IdP bliver afkoblet Unilogin Broker."

Unilogin Broker er en bestemmende komponent for SkoleLogin – fra og med 1. marts 2023. Det er en indirekte deadline, da den forudsætter NSIS godkendelse.
Ligeledes skal kommunerne NSIS-godkendes, hvis en lokal idP skal benyttes i forbindelse med overgangen fra NemID medarbejdersignatur til MitID Erhverv.
Af en oversigt fra Digitaliseringsstyrelsen er der ni NSIS-godkendte kommuner.

Af Stine Page, Connector A/S og Kaare Pedersen, Lead – enter next level

Vi har brug for digitaliseringskonsulenter med jord under neglene

Digitaliseringskonsulenters er brobyggere mellem teknologierne og ledere og medarbejderes hverdag. De skal både oversætte den ene vej, fra teknologierne til lærernes, pædagogernes, sagsbehandlernes hverdagspraksis og den anden vej fra praksis til teknologi.

Behov i hverdagen med borgerne kan dog sjældent løses fra skrivebordet og derfor skal digitaliseringskonsulenterne ud i marken, få jord under neglene og få førstehåndsindsigt i den praksis, som skal understøttes digitalt. Det lyder selvfølgeligt, at man skal tæt på. Men er det praksis? Sker det nok? Og hvad holder os eventuelt tilbage?
I det følgende giver vi eksempler på, hvor vi har oplevet at tæt samarbejde mellem digitaliseringskonsulenter og fagpersoner har haft stor betydning – og hvorfor det kan være svært i praksis at bevæge sig ud af kontorerne.

Hvorfor skal vi gå en længere tur i marken?

Uanset hvor et digitaliseringsinitiativ kommer fra, er der brug for at se og formidle behov og muligheder mellem brugere og leverandører. Det kræver en som regel en kompleks udveksling af viden mellem parterne, allerhelst i form af samtaler, hvor man får hjælp til at forstå hinanden på tværs af digitaliseringsfaglighed og fag-fagligheder.
Kvaliteten af kontakten er afgørende, sammen med evnen til at sætte sig ind i den praksis, det digitale skal understøtte. Mange steder foregår det på skrift, i møder eller på workshops om brugernes behov. Vi vil dog advokere for en endnu tættere kontakt: at digitaliseringskonsulenten går i marken, stiller sig brugernes sko og går vejen sammen med dem. F.eks ved at være med i hverdagen i en uges tid. Det kan være i arbejdet med en sag fra A-Z på tværs af enheder, eller i det pædagogiske arbejde med en borger, hvor det digitale skal styrke den faglige praksis. Konsulentens opgave er at forstå og sætte ord på brugernes hverdag, så man sammen kan bringe fagligheder i spil og få øje på

muligheder og potentialer, som grundlag for at definere krav til nye løsninger.
Når løsninger skal implementeres, er der igen brug for den tætte kontakt med fødderne i mulden. At man med egne øjne ser, hvordan anvendelsen af teknologien udspiller sig.
I en kommune, hvor den ene af os skulle hjælpe en implementering med mange udfordringer, indførte vi et princip: Vi taler aldrig om et problem uden at se det live. Vi så altid problemerne direkte i det digitale redskab, og kunne ofte løse dem, fordi en deltager kendte en metode.
I en anden kommune arbejdede en af os med en prototype-tilgang, hvor den digitale løsning blev udviklet gennem brugernes erfaringer. Da digitaliseringen også var en faglig forandring, måtte konsulenter og brugere følges tæt ad, for at forstå og identificere behov og faglige muligheder sammen i takt med, at de kom til syne gennem det nye redskab. Her var det tætte praksisnære samarbejde afgørende for, at løsningen blev enkel, intuitiv og fagligt meningsfuld.
Det samme gælder, når man skal optimere eksisterende løsninger. Nogle gange bruges løsningerne måske med gamle arbejdsgange, og derfor opnår man ikke værdien. Her kan opgaven for konsulenten være at udforske både det der virker, og det der bøvler. Det man taler meget om, og det der måske er tavs viden. Eller viden, der ikke er til stede om, hvordan systemet skal anvendes for, at de indbyggede funktioner og muligheder fungerer efter hensigten. Det har vi set i en kommune, hvor man pga. 'gammel adfærd' i det nye system, ikke fandt den viden, man havde brug for, og derfor ikke oplevede at det digitale styrkede samarbejdet og havde værdi.

Nemt, men ikke så nemt alligevel

En ting er at aftale at vi skal have jord under neglene. Noget andet er at gøre det. At ændre sin måde at arbejde på, sine daglige prioriteter.
Kegan og Lahey taler om "Hidden competing commitments", altså skjulte eller usagte konkurrerende forpligtigelser, der bremser os i at gøre det, vi gerne vil. De kan hvile på grundlæggende antagelser, der både kan være rigtige og skævvredne.
- se figur nederst på siden.
De fleste kan sikkert genkende, når man har besluttet at gøre noget nyt – og så sker det alligevel ikke. Det er her, vi skal kigge på de skjulte og konkurrerende forpligtigelser. Hvad er det der – bevidst eller ubevidst – trumfer vores "hellige ild"? Som alligevel virker tungere i hverdagen? Hvilke grundlæggende antagelser hviler de på? Om os selv, om vores afdelings mål og succeskriterier? Og om vores samarbejdspartnere?
Det kan både være grundlæggende antagelser hos os selv og andre, som står i vejen. Nogle bunder i organisationskultur og ledelse, andre i vores egen opfattelse af roller og opgaver, styrker og frygt.


Stine Page

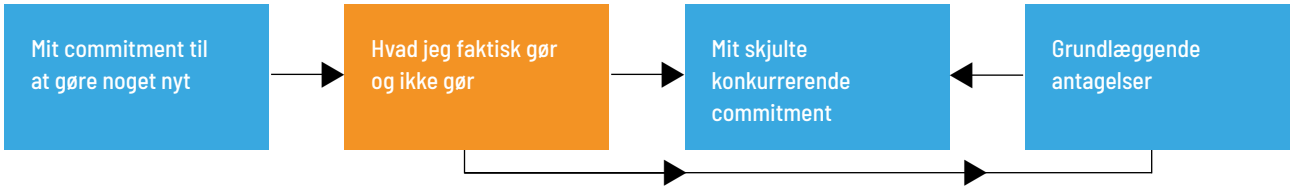

Kaare Pedersen

Det kan f.eks handle om opfattelser af, at digitaliseringskonsulenter tager sig af det tekniske, og at de kommer med løsninger, der ikke kan diskuteres, og at de mere er nogle, der fikser end lytter. Og i IT-afdelingen kan en skjult antagelse være, at det er ineffektivt at bruge så meget tid hos brugerne. Den lader vi stå.
For digitaliseringskonsulenten selv kan det opleves usikkert at begive sig ud i de mere antropologiske processer, hvor man ikke skal finde svar, men skal holde igen på trangen at finde en løsning. Det kan være ubehageligt at stå alene hos brugerne og stille spørgsmål ind i sit eget fagområde, som man ikke kender svaret på. Der er en lang bevægelse i den faglige selvforståelse fra at være ekspert i GDPR og RPA, til at gå på opdagelse i hverdagen hos en daginstitution eller et botilbud i psykiatrien. Og udfordre sin egen og brugerens forventninger om, at man altid har svar.
Så selvom vi kan tale om, at konsulenten skal ud at skabe værdi i organisationen helt tæt på hverdagen, kan de skjulte forpligtigelser eller grundlæggende antagelser trumfe og gøre, at prioriteringen af opgaverne alligevel lander på arbejdet med it-systemerne ved skrivebordet.

Hvad kan I gøre?

At skulle lytte og forstå behov, som kræver udveksling af viden , kan altså være nyt land for alle parter. Det kalder derfor på samtaler om, hvad man har brug for fra hinanden, for at lykkes med digitaliseringen som en fælles opgave.
Er du chef for digitaliseringskonsulenter er vores anbefaling, at du sætter drøftelser af, hvad der har betydning og værdi for at lykkes med digitaliseringen på dagsordenen. Og hvorfor digitalisering kræver en brugerforståelse, som har brug for tid til at udvikle sig i gensidighed. Der kan både være behov for at drøfte roller og prioriteringer internt i enheden. Og for at drøfte det med dine chef-kolleger fra andre afdelinger, for at fremme forståelsen for at digitalisering er et samarbejde, som kalder på at konsulenterne kommer tæt på. Forklar f.eks. hvad det konkret indebærer – at I kommer på besøg, er med, ikke skal finde svar, men sammen afdække behov og muligheder først.
Og endelig – skab rum for at dine medarbejdere kan lufte deres usikkerhed og udveksle erfaringer. Træn brug af enkelte antropologiske redskaber og perspektiver, og gå med hinanden ud i marken. Inviter f.eks brugere med til en dialog om, hvordan man kan tale og forstå hinanden med forskellige faglige sprog. Følg op, stil spørgsmål og vær vedholdende. Og vov at evaluere på, om brugerne oplever, at jeres besøg gør en forskel.

«««



NY SKI-AFTALE PÅ IT-DRIFT GIVER DIG FLEKSIBILITET OG BREDDE

It-drift dækker over forskelligartede og komplekse løsninger – og behovet hos kommunerne er meget individuelt.

På 02.22 It-drift kan du fra januar 2023 købe it-drift og relaterede services i et dynamisk indkøbssystem.

Det betyder, at:

- Du får fleksible rammer for dit indkøb af it-drift uden fast definerede services
- Du kan skræddersy dit indkøb – uanset om du ønsker drift af en enkelt server eller outsourcing af hele din it-drift
- Nye leverandører løbende kan optages – og byde ind med nye muligheder.

Dit indkøb i det dynamiske indkøbssystem bliver samtidig understøttet digitalt: Du vælger og stiller krav i vores digitale flow, der automatisk genererer det relevante udbudsmateriale til dit indkøb. Det gør indkøbet nemmere fra start til slut – for både dig og de leverandører, der kan afgive tilbud.

Vil du vide mere om dine muligheder med den nye aftale 02.22 It-drift, så kontakt os.

Kontakt

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

Tobias Lundquist
Kontraktansvarlig
T - 20 62 46 48
E - tlu@ski.dk

Staten og Kommunernes Indkøbsservice A/S · Montagehallen, Pakkerivej 6 · 2500 Valby · Telefon +45 33 42 70 00