Det kommunale perspektiv

- med et grønt twist

KL Dialogforum

Henrik Brix, Favrskov Kommune og formand for KITA

4. maj 2023, KL-huset

KITA
Kommunale IT- og Digitaliseringsansvarlige

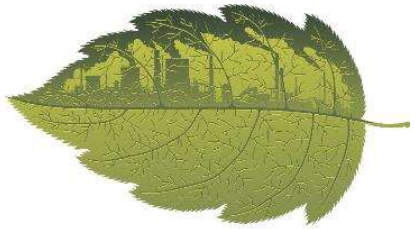
Det kommunale perspektiv

Aktuelle udfordringer på digitaliseringsområdet, med særligt fokus på grønne indkøb

- NSIS

- Cybersikkerhed
  - Herunder tredjelandsoverførsler

- Grønne indkøb – grønt fokus



KITA
Kommunale IT- og Digitaliseringsansvarlige

NSIS
National Standard for Identiteters Sikringsniveauer

- Fylder i alle kommuner – vi har travlt
- Procedurer, teknisk løsning, revision, godkendelse, certifikater, implementering…
- En kort tur til Favrskov

Betydelig	3)Det Elektroniske Identifikationsmiddel skal gøre brug af mindst to Autentifikationsfaktorer fra forskellige kategorier.	Det elektroniske identifikationsmiddel består af 2 forskellige typer af autentifikationsfaktorer: •Kodeord (videns baseret autentifikationsfaktor) •2-faktor enheder (ihændehaverbaseret autentifikationsfaktor) Favrskov Kommune anvender følgende 2-faktor enheder: •MitID privat (valgfrit for IT-brugeren) •OS2faktor authenticator app •Kodeviser OS2faktor hændelseslogger alle anvendelser af identifikationsmidler, hvor man kan se typen af autentifikationsfaktor anvendt.	* Procedure for elektronisk identifikationsmiddel * Risikovurderinger og argumentation * Skærmprint med oversigt over MFA-tilknytninger i OS2faktor * Brugerkonti-log i OS2faktor Kontrol i Wired Relations: NSIS 3.3.1-4 Gennemgang af beskrivelser mv. i leverandørens revisorerklæring
	4)Det Elektroniske Identifikationsmiddel er udformet således, at det kan antages, at det kun kan bruges, når det er den person, som det tilhører, der har kontrol over og er i besiddelse af det.	Ud fra Digital Identitys ISAE 3000 NSIS-revisionserklæring vurderes dette punkt at være opfyldt i OS2faktor løsningen, idet der anvendes 2-faktor enheder, der kræver fysisk besiddelse.	* Seneste ISAE 3000 NSIS revisionserklæring fra Digital Identity samt dokumentation for tilsyn af samme * Risikovurderinger og argumentation Kontrol i Wired Relations: NSIS 3.2.2 Gennemgang af auditlogs i OS2faktor NSIS 3.3.1-4 Gennemgang af beskrivelser m.m. i leverandørens revisorerklæring

Overgangen til MitID Erhverv går ind i den afsluttende fase 30. juni 2023

27-04-2023

Alle virksomheder, myndigheder og foreninger, der anvender NemID til erhverv skal skifte til MitID Erhverv, inden NemID til erhverv lukker.

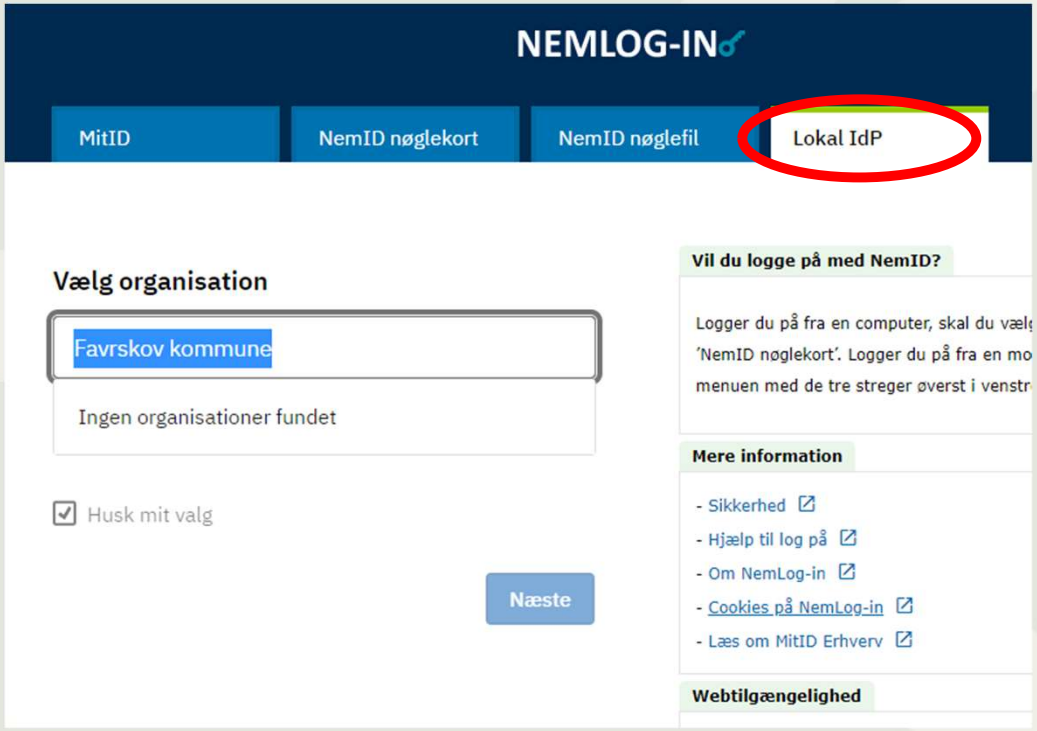
For at sikre en god og sikker overgang for centrale og komplekse løsninger og organisationer, fx kommuner og regioner, vil NemID til erhverv ikke som planlagt lukkes fuldt ned den 30. juni 2023, men fortsætte med begrænset drift og afvikles gradvist frem til den 31. oktober 2023.

Skift fra NemID Medarbejdersignatur til MitID Erhverv

- **Krav** om øget sikkerhed for brugeridentiteter (NSIS) fra 1. ~~juli~~ november 2023
- **Krav** om **to-faktor-login** visse steder
- I forbindelse med skiftet skal ***alle 3.300*** **it-brugere verificeres** (kommunen skal sikre sig, at du er dig) ved brug af ***personligt*** **MitID**
- 1.260 it-brugere anvender i dag NemID medarbejdersignatur til fx AULA og Fælles Medicin Kort
  - Skal vælge to-faktor enhed

Favrskov Kommune

Nye vaner – stor implementeringsopgave



Favrskov Kommune

Cybersikkerhed

- Alle taler om det
- Eksemplerne står nærmest i kø (mest DDOS (endnu))

- Foran hoveddøren står
  - Politi, forsvar m.m.

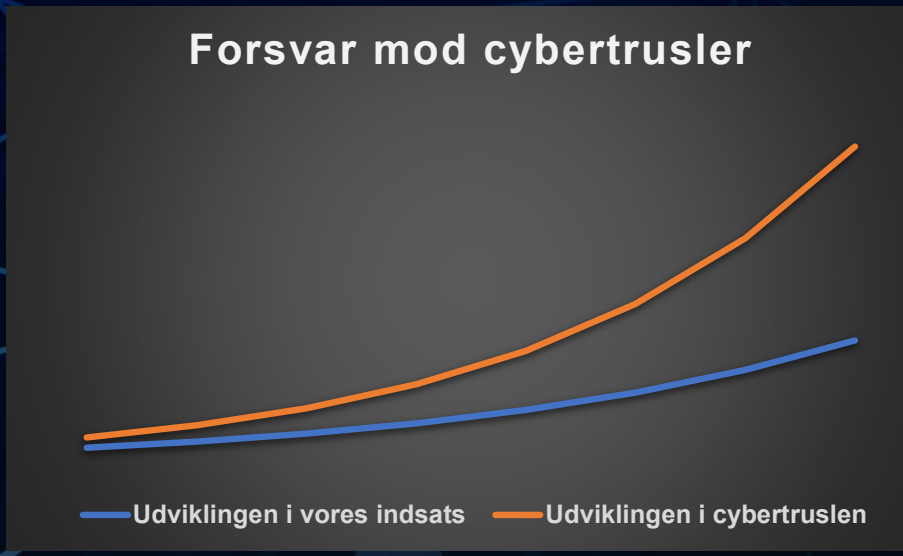
- Foran den digitale hoveddør…
  - Er vi noget alene

- Kalder på øget indsats og samarbejde
  - Både mellem kommuner og med leverandører.

Cybersikkerhed – behovet i fremtiden

- Trusselsniveauet (kapacitet x intention) stiger (falder det igen?)
- Cloud-tjenester kræver yderligere opmærksomhed
- Samarbejde med andre sektorer
  - Fx sundhedsområdet (DCIS Sund)
  - Vil stille yderligere krav
- Øget behov for 24/7 overvågning
- Øget opmærksomhed og forventninger

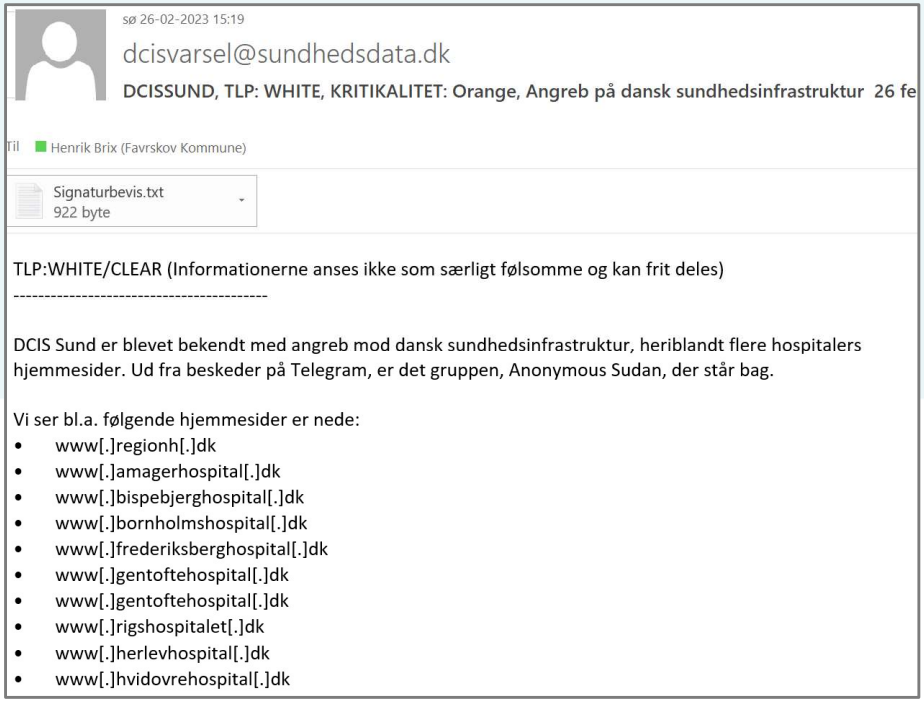
- **Vi kommer til at hæve niveauet**



Øgede krav udefra, fx

- Aftale om samarbejde med DCIS Sund
  - Overvågningsbokse (NDR) i alle 98 kommuner
  - Varsler om angreb/hændelser/sårbarheder
  - Dækker alene ansatte indenfor sundhed
  - 24/7 forventning

- Måske flere sektorer.



sø 26-02-2023 15:19

dcisvarsel@sundhedsdata.dk

DCISSUND, TLP: WHITE, KRITIKALITET: Orange, Angreb på dansk sundhedsinfrastruktur 26 fe

Til Henrik Brix (Favrskov Kommune)

Signaturbevis.txt
922 byte

TLP:WHITE/CLEAR (Informationerne anses ikke som særligt følsomme og kan frit deles)

DCIS Sund er blevet bekendt med angreb mod dansk sundhedsinfrastruktur, heriblandt flere hospitalers hjemmesider. Ud fra beskeder på Telegram, er det gruppen, Anonymous Sudan, der står bag.

Vi ser bl.a. følgende hjemmesider er nede:

- www[.]regionh[.]dk
- www[.]amagerhospital[.]dk
- www[.]bispebjerghospital[.]dk
- www[.]bornholmshospital[.]dk
- www[.]frederiksberghospital[.]dk
- www[.]gentoftehospital[.]dk
- www[.]gentoftehospital[.]dk
- www[.]rigshospitalet[.]dk
- www[.]herlevhospital[.]dk
- www[.]hvidovrehospital[.]dk

Øgede krav udefra - fortsat

- NIS2 – øgede krav til sikkerhed og ansvar
  - Endnu ikke besluttet om kommunerne omfattes
- Øget tilsyn med fx kontrol af adgange og log (Datatilsynet)
- Tekniske minimumskrav – Staten og KL
  - Kommunerne er ikke sådan rigtig omfattet
  - Men Datatilsynet opfatter det som krav

K1	For borger-PC'er gælder det, at tilslutning af eget udstyr skal blokeres fysisk og ved krav om administratortilladelse.	Her tænkes fx på PC'er, der opstillet på biblioteker eller andre offentlige steder med fri tilgængelighed for borgerne. Formålet er beskyttelse mod keyloggere eller anden skadelig software samt misbrug af kommunens systemer og ressourcer.	Best practice
K2	Der skal opsættes en politik for konfiguration af PC'er uden password (fx borger-PC'er), som tilgodeser brugernes sikkerhed i størst muligt omfang.	Borgere skal kunne være trygge ved at benytte kommunens opstillede PC'er. En fysisk sikret tynd klient, med et sikret OS, hvis virtuelle maskine nulstilles efter hver session, ville være idéelt.	Best practice

K8	Ekstern adgang til eksempelvis konsulenter skal tildeles tidsbegrænset og kun til og med opgavens ophør. Den eksterne adgang skal kun inkludere adgang til relevante systemer/services ift. den konkrete opgaveløsning.	Eksterne brugere skal benytte multifaktor autentifikation hvor muligt og kun have tidsbegrænset adgang til det nødvendige.
K9	Passwords skal udformes, opdateres og opbevares i overensstemmelse med CFCS anbefalinger	At medarbejdere ikke benytter usikre kodeord og at brugeroplysninger ikke kan tilgås af utilsigtede.

Nr.	Klienter/PCer		
	Anbefaling	**Uddybning**	**Følger af**
S1	Der skal implementeres firewall på alle klienter.	Firewalls skal sikre mod utilsigtet adgang til arbejdsstationer. Malware forsøger typisk at sprede sig på tværs af systemer, og ved at fjerne denne mulighed kan man begrænse denne spredning. Bør konfigureres så restriktivt som muligt.	Best practice
S2	Der skal benyttes en af kommunen stillet til rådighed VPN-løsning eller anden sikkerhedsteknologi, der tilgodeser krav til autentifikation af brugeren og kryptering af data til at tilgå kommunens systemer og ressourcer via arbejds-PC fra eksterne netværk.	Brug af VPN eller anden sikkerhedsteknologi skal sikre dataintegritet og fortrolighed og bl.a. modvirke man-in-the-middle angreb.	CFCS: It-sikkerhed på rejsen
S3	Alle harddiske på til medarbejdere udleverede enheder skal krypteres efter tidssvarende standard.	For at undgå kompromittering af data i forbindelse med tab eller tyveri af pc, skal operativsystemet være sat op til at kryptere harddisken på den enkelte enhed.	CFCS: It-sikkerhed på rejsen

Leverandørernes – jeres – rolle/opgave

- Ca. 3/4 af kommunale systemer er outsourcet!
- Vi kan ikke hæve niveauet uden jer
- NDR bokse hos leverandører?
- 24/7 overvågning/kontakt?
- Implementering af NSIS krav i løsningerne?
- Håndtering af sikkerhedshændelser – ok?
- Mulighed for kontrol af adgange og log?
- Sletning (og arkivering) af data?
- …
- Øgede krav i kontrakter og aftaler.

KITA
Kommunale IT- og Digitaliseringsansvarlige

Tredjelandsoverførsler

Det er ikke rigtig blevet nemmere…

Datatilsynet udskyder afgørelse i Chromebook-sag

GDPR | 13. december 2022 kl. 10:41 | 7

OMPLIANCETECH

Artikler Synspunkter Om Mere

GDPR Databeskyttelse AI Act EU Offentlig digitalisering Lovgivning Algoritmer Chatbot Jura

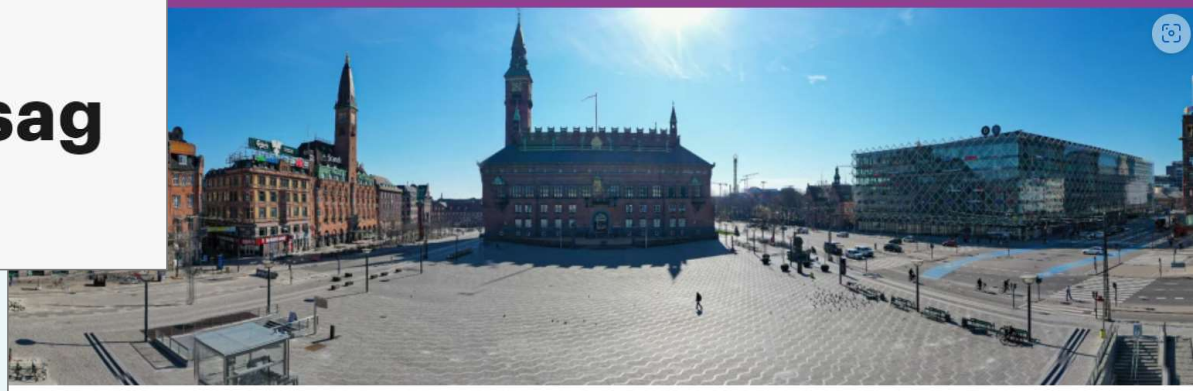
Tyske datatilsyn rammer Microsoft: Myndigheder må ikke bruge Office 365

GDPR | 13. december 2022 kl. 05:00 | 13

COMPUTERWORLD

CIO TECH EKSPERTEN IT-JOB IT-KURSER EVENTS PODCAST SØG

HVAD ER PREMIUM? PREMIUM FAQ KONTAKT DIT ABONNEMENT



(Foto: Lars Jacobsen)

Københavns Kommune tager europæisk cloud-alternativ i brug: "Det tegner til, at den virkelig kan noget på både funktionalitet og pris"

Interview: En europæisk cloud-platform er begyndt at snurre i Københavns Kommune, der i kølvandet på Schrems II-dommen måtte indstille overgangen til Microsoft Azure. Der er spændende perspektiver i den nye platform, lyder det fra Koncern IT's direktør Kristina Skovdal.

Grønt fokus?

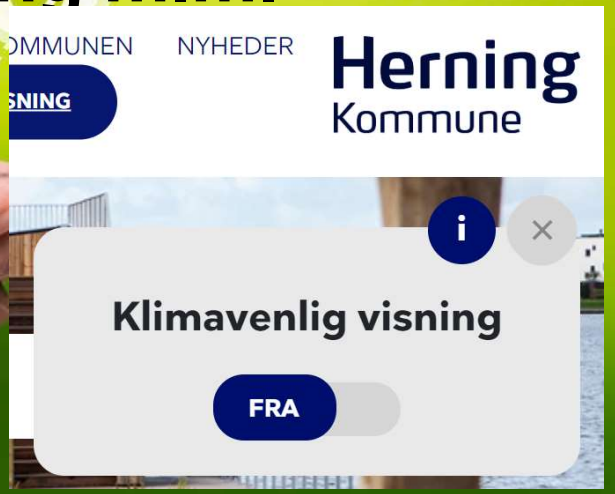
- ”Højt” prioriteret på den politiske agenda lokalt, men…
- Noget forskelligt fra kommune til kommune
- Det tager tid
- Slået lidt ”hjem” af krigen og forsyningssikkerhed og cybersikkerhed og NSIS og …

Grønt fokus

- MEN det kommer!
- Gør det meget synligt/dokumenterbart
  - Ikke bare sandsynligt
- Det må ikke være (ret meget) dyrere
  - Nemmere at acceptere, at der skal investeres for så at få en gevinst senere - men så skal det også være der

Grønt fokus – mange aspekter

- HW – fx genbrug/holdbarhed, strømforbrug og klimaaftryk
- SW – fx strømforbrug ved afvikling, SW til ruteplanlægning/ flådesammensætning m.m.
- Varmegenvinding fra datacentre
- Regulering?



Jeg kunne også have nævnt...

- Arbejdskraftmangel
  - Arbejdskraftreducerende digitalisering
- Bedre/yderligere brug af den fælleskommunale infrastruktur
- Brug af kunstig intelligens i kommunerne
- It- og digitaliseringschefernes rolle
  - Digitalisering flytter ”hjemmefra” og ud på velfærdsområderne
  - Definere vores rolle i det
  - Hvordan undgår vi at blive nej-kontoret?

KITA

Kommunale IT- og
Digitaliseringsansvarlige