KS Team for Direktionsbetjening KS og KIT (5900)
Økonomiforvaltningen

Notat

Til Emil Moselund (B)

11-02-2022

Sagsnummer i F2
2022 - 1812

Dokumentnummer i F2
888621

Sagsnummer eDoc
2022-0040212

Svar på spørgsmål vedrørende implementerede initiativer for at opjustere den digitale it-sikkerhed

Den 30. januar fremsendte Emil Moselund (B) nedenstående spørgsmål skriftligt til Borgerrepræsentationens Sekretariat.

1. *Kan forvaltningen redegøre for hvilke initiativer man fra 2018-2021, har implementeret for at opjustere den digitale IT-sikkerhed?*

2. *Ift. regeringens "Nationale Information og Cyber-strategi" ligger der en række krav til de offentlige myndigheder, som skal implementeres. Har Københavns Kommune planer ift. denne strategi, der delegerer yderligere opgaver ud til det offentlige?*

3. *Endvidere vil jeg gerne vide, hvor den juridiske grænse går ift. det kommunale ansvar vs. det statslige ansvar for egen sikkerhed? Her særligt med fokus på Energi og netværks-installationer, affaldssektoren, varmeforsyning, og beredskabet.*

Økonomiforvaltningens svar

Svar på spørgsmål 1
Økonomiforvaltningen forudsætter, at der med spørgsmålet ønskes svar på de tekniske og cybersikkerhedsmæssige forhold af betydning for it-sikkerheden i Københavns Kommune (KK).

Økonomiforvaltningen har i perioden 2018-2021 iværksat en lang række initiativer med henblik på at øge den digitale (tekniske) it- og cybersikkerhed i KK.

Udvalgte af de iværksatte initiativer fordeler sig på følgende kategorier:

1. Governance
2. Cybersikkerhed
3. Beskyttelse af it-brugere og deres it-udstyr
4. Sikkerhed i it-systemer.

De fire ovenstående kategorier er kort udfoldet nedenfor:

Ad.1: Governance
I 2018 besluttede Borgerrepræsentationen en ny og stærkere governance for it-området. På den baggrund nedsatte man en IT-kreds bestående af de digitaliseringsansvarlige direktører i hver forvaltning samt direktøren for Koncern IT. Målet var bl.a. at etablere en sikkerhedskreds, der overvåger, koordinerer og giver input til kommunens overordnede it-sikkerhedsfunktion i Økonomiforvaltningen (ØKF).

Ad.2: Cybersikkerhed
For perioden 2018 – 2021 har KK oprustet arbejdet med cybersikkerhed markant. Der er etableret målrettet opsamling af logfiler fra både fagsystemer og fra it-infrastrukturen, hvilket sikrer en bedre kontrol af, om uvedkommende tilgår KK-systemer. KK har desuden implementeret en styrket monitorering og etableret en fast proces for simulerede cyberangreb (penetrationstest). Endelig har KK opdelt den samlede it-installation, så et potentielt vellykket hackerangreb ikke kan sprede sig til hele installationen.

Ad.3: Beskyttelse af it-brugere og deres it-udstyr
Siden 2018 har ØKF sikret øget beskyttelse af alle it-brugere i KK. Der er indført øget sikring af brugernes passwords, herunder sikker mulighed for skift af disse med NemID samt anvendelse af to-faktor godkendelse. Der er gennemført awareness-kampagner med løsningen 'Hoxhunt', der træner medarbejdere i at gennemskue phishing, og sikkerheden på it-brugernes it-udstyr er ligeledes forbedret med nye procedurer for opdateringer af enhedernes styresystemer og applikationer samt sikring af enhederne med kryptering af harddiske og antivirus. Corona-krisen har medført en særlig indsats, hvor et meget stort antal medarbejdere måtte anvende deres it-udstyr hjemmefra. I den anledning har KK iværksat særlige indsatser med fokus på sikkerheden i hjemmenetværk, fjernopdateringer af it-udstyr og kommunikation om it-sikkerhed ved hjemmearbejde.

Ad.4: Sikkerhed i it-systemer
ØKF har på en række områder øget sikkerheden i KK's samlede portefølje af it-systemer. Der gennemføres årlige risikovurderinger af udvalgte systemer, som suppleres af tilsyn med opfølgning på henstillinger. ØKF har udarbejdet en række standarder for blandt andet kryptering, dataopbevaring, logning og brug af to-faktorgodkendelse i perioden fra 2018 til 2021. Hertil skal det fremhæves, at tildelingen af adgange og ledelsestilsyn med disse er under automatisering og yderligere sikring på KK's nye adgangsstyringsplatform, hvor der med udgangen af 2021 var tilkoblet ca. 160 ud af 240 udvalgte systemer.

Svar på spørgsmål 2
Regeringens 'Nationale strategi for cyber- og informationssikkerhed' indeholder en række strategiske målsætninger for en stor del af de statslige myndigheder og alle ministerområder. Strategien forholder sig imidlertid ikke til arbejdet med cyber- og informationssikkerhed på det kommunale område.

ØKF følger imidlertid løbende udviklingen i sikkerhedsanbefalinger fra Center for Cybersikkerhed (CFCS), og Københavns Kommunes årlige trusselsvurdering baserer sig bl.a. på anbefalinger fra CFCS og en række øvrige kilder.

Desuden anvender Økonomiforvaltningen de "20 tekniske minimumskrav for statslige myndigheder", der er godkendt af styregruppen for den nationale cyber- og informationssikkerhedsstrategi som benchmark til indsatsen i Københavns Kommune.

Svar på spørgsmål 3
Økonomiforvaltningen forudsætter, at der med spørgsmålet ønskes svar på, hvilket ansvar en kommune har i forhold til it-sikkerhed i forsyningssektoren.

Forsyningssektoren er reguleret i en lang række love og bekendtgørelser, hvori der også ofte er en nærmere regulering af beredskab i forbindelse med fx krisesituationer, da forsyningssektoren anses som samfundskritisk.

Det er ikke muligt inden for rammerne af et politikerspørgsmål udtømmende at give en beskrivelse af, hvilken lovgivning der regulerer forsyningssektoren. Overordnet kan det oplyses, at forsyningssektoren, herunder beredskabet, er reguleret i love og bekendtgørelser, som er udstedt af staten. Fx er det Energistyrelsen, der udarbejder den lovgivning, som fastsætter rammerne for beredskabet i sektorerne el, naturgas, bygas, olie og fjernvarme.

Lovgivningen angiver, hvordan sektoren er organiseret, og herunder hvem der har ansvaret for beredskabet. Forsyningssektoren er i vidt omfang organiseret i selskaber, som kommunerne har ejerskab i. Det er selskabernes ansvar, at der er det nødvendige beredskab til at opretholde forsyningen i tilfælde af en krise, herunder også i forhold til it-sikkerhed.

Økonomiforvaltningen har været i dialog med KL, som oplyser, at der i forbindelse med udarbejdelsen af den nye nationale strategi for cyber- og informationssikkerhed ikke har været nogen overvejelser om en ny ansvarsfordeling i forhold til de kommunale opgaver. Hertil skal det bemærkes, at det forsat ligger inden for fagministeriernes kompetencer at stille krav til kommunerne via ny regulering. Det kan således ikke afvises,

at den nye nationale strategi for cyber- og informationssikkerhed på et senere tidspunkt vil medføre nye krav til landets kommuner.