KIT Sikkerhed 2 (5953)
Økonomiforvaltningen

Orienteringssag

Til Økonomiudvalget

Orienteringssag til Økonomiudvalget "Status på informationssikkerhedsområdet 2021"

06-05-2022

Sagsnummer i F2
2022 - 3383

Dokumentnummer i F2
1014273

Sagsnummer eDoc
2022-0073880

Sagsbehandler
Camilla Lundgren-Eliasen

Resumé
Økonomiforvaltningen orienterer Økonomiudvalget om status på informationssikkerhedsarbejdet, dispensationer fra Københavns Kommunes informationssikkerhedsregler og informationssikkerhedsbrud i kommunen mindst én gang årligt, som det fremgår af forretningscirkulære for organisering af informationssikkerhed § 4, stk. 4. I 2021 er der gennemført en række indsatser, der imødegår truslerne mod kommunens generelle drifts- og datasikkerhed. Det er Økonomiforvaltningens vurdering, at de kendte sikkerhedsrisici for kommunens it-systemer befinder sig på et acceptabelt niveau, samt at det nuværende beskyttelsesniveau af kommunens it-infrastruktur generelt ligger på et passende beskyttelsesniveau.

Sagen forelægges til orientering.

Problemstilling
Arbejdet med at sikre en høj informationssikkerhed tager afsæt i en årlig trusselsvurdering, som Koncern IT foretager, samt i konklusionerne fra de tilsynsaktiviteter og risikovurderinger, som Databeskyttelsesrådgiveren og Koncern IT gennemfører årligt. Ekstern Revision fører ligeledes tilsyn med Københavns Kommunes organisering af informationssikkerhed.

Indsatsen på informationssikkerhedsområdet planlægges ud fra en risikobaseret tilgang, og der foretages dermed en afvejning mellem sikkerhedsmæssige risici og kommunens behov for effektivitet og høj borgerservice. Dette skal sikre, at enhver håndtering af personoplysninger og værdioplysninger i Københavns Kommune sker på en betryggende og tillidsvækkende måde i forhold til kommunens borgere og virksomheder, og at kommunen følger gældende databeskyttelsesregler for behandling af personoplysninger.

Det er Økonomiforvaltningens vurdering, at de kendte sikkerhedsrisici mod kommunens it-systemer befinder sig på et acceptabelt niveau,

samt at det nuværende beskyttelsesniveau af kommunens it-infrastruktur generelt ligger på et passende beskyttelsesniveau.

Løsning

Trusselsvurdering
Koncern IT opdaterer kommunens trusselsvurdering på cyberområdet én gang årligt. Cybertruslen mod Københavns Kommune er fortsat meget høj. Flere angreb i 2021 understreger den alvorlige internationale udvikling, der også i Københavns Kommune kræver et stort fokus på cyberforsvaret. I 2021 har tre trusler haft særlig fokus.

1. Ransomware-angreb
Ransomware-angreb er afpresningssoftware, der kan forhindre kommunens adgang til egne data og hardware med krav fra ondsindede cyberkriminelle om løsepenge for frigivelse og adgang til egne data. Årsagen til den øgede trussel på området udspringer bl.a. af, at mange medarbejdere under covid-19 krisen primært har arbejdet hjemmefra på usikre private netværk. Gennem skadelige links i phishingmails har cyberkriminelle forsøgt at udnytte den svagere beskyttelse. Københavns Kommune bliver dagligt ramt af forsøg på phishing men har implementeret en række forsvarsmekanismer, som indtil videre har forhindret alvorlige angreb.

2. Angreb via leverandørsoftware
Angreb via leverandørsoftware var en ny trussel i 2021. Der er set flere eksempler på, at cyberkriminelle har skaffet sig adgang til organisationer gennem sikkerhedshuller i leverandørsoftware. Konkret blev Københavns Kommune og andre større organisationer ramt via et netværksprodukt, hvor russiske statshackere havde en bagdør til kommunens netværk, dog uden at det medførte tab eller kompromittering af data for Københavns Kommune. Sagen er et eksempel på den stigende trussel på cyberområdet.

3. Utilsigtede angreb
Endelig er truslen fra utilsigtede angreb forsat meget høj. Disse utilsigtede destruktive cyberangreb er ikke målrettet Københavns Kommune, men kan alligevel ad omveje ramme kommunen gennem malware eller ransomware. Der er set meget alvorlige tilfælde af denne type incidents i Danmark i 2021. Den tilspidsede situation på baggrund af krigen i Ukraine, hvor parterne anvender cyberangreb, øger risikoen for utilsigtede angreb.

Centrale initiativer til sikring af informationssikkerheden 2021
Økonomiforvaltningen har i samarbejde med kommunens øvrige forvaltninger igangsat og implementeret en række initiativer til sikring af informationssikkerheden i 2021.

1. Cyberforsvar
Som del af *Cyberpakke 1*, der blev vedtaget af Økonomiudvalget i 2018, blev der iværksat en række tiltag til forbedring af Københavns Kommunes cybersikkerhed i forhold til det på tidspunktet gældende trusselsbillede. Siden 2018 har cybertruslen mod Københavns Kommune været stigende og vurderet som "meget høj", og der konstateres løbende nye og avancerede hackerangreb, som kommunen skal beskytte borgernes data og egne it-installationer imod.

Derfor har Økonomiforvaltningen igangsat et arbejde på en *Cyberpakke 2*, så Københavns Kommune fortsat kan stå imod det aktuelle og stigende trusselsbillede. Indsatserne i *Cyberpakke 2* vil bestå af de tiltag, som vurderes at have den største effekt på cybersikkerheden i kommunen. Tiltagene vil blive drøftet i kommunens kreds af de it-ansvarlige direktører forinden politisk behandling.

Den aktuelle situation i Ukraine har medført et øget fokus på cybertruslen. Der ses en øget aktivitet fra kendte russiske ip-adresser, som anvendes til ulovlig cyberaktivitet rettet mod kommunens infrastruktur, og der rapporteres allerede om virksomheder i Danmark, som er blevet ramt. Center for Cybersikkerhed har anbefalet en række tiltag, som myndigheder og virksomheder kan bruge til at styrke deres cyberberedskab. Det er vurderingen, at Københavns Kommunes infrastruktur og beredskab generelt lever op til disse tiltag, og at kommunen er godt forberedt på den nuværende situation. På grund af den aktuelle situation har Økonomiforvaltningen:

- Skærpet monitoreringen af kommunens it-infrastruktur ved at implementere yderligere monitorering på servere, der er eksponeret mod internettet
- Intensiveret samarbejdet med Center for Cybersikkerhed, DCIS-Sund og private it-sikkerhedsfirmaer i forhold til udviklingen i trusselsniveauet
- Foretaget en ekstraordinær gennemgang af reetableringsplaner for kommunens it-infrastruktur, så de er helt opdaterede i tilfælde af en alvorlig cyberhændelse.
- Udsendt en status til forvaltningerne via kommunens it-ansvarlige direktører og digitaliseringschefer over Økonomiforvaltningens tiltag samt en anbefaling om, at forvaltningerne opdaterer og evt. afprøver forvaltningsspecifikke planer for fortsat drift uden it-understøttelse.

Økonomiforvaltningen kommunikerer løbende om god skik ift. at agere sikkert i kommunens it-systemer og gennemfører løbende kampagner og øvrig awareness for at skærpe brugernes opmærksomhed herom. Formålet er dels at gøre opmærksom på phishing-forsøg, hvor cyberkriminelle forsøger at franarre brugerne person- eller værdidata, eller få brugerne til at klikke på ondsindet kode, og dels vigtigheden af at holde pc'ere og telefoner opdaterede.

2. Sikkerhedstiltag som følge af Covid-19
Som følge af covid-19 krisen har Koncern IT iværksat og vedligeholdt flere målrettede indsatser, der blev igangsat i 2020 ved pandemiens begyndelse. Koncern IT har fortsat den målrettede kommunikation til it-brugerne i et tæt samarbejde med både Økonomiforvaltningen og Digitaliseringschefkredsen.

Koncern IT tilrettede i den helt tidlige fase af covid-19 pandemien kommunens sikkerhedsmonitorering af netværket til den nye situation med hyppig brug af hjemmearbejde. Den primære tilpasning har været til det nye brugsscenarie, hvor mange flere medarbejdere har arbejdet hjemmefra og derfor har skulle tilgå kommunens it-infrastruktur fra ydersiden. Det har også betydet, at Københavns Kommune har haft fokus på at sikre den nødvendige kapacitet til sikre og krypterede adgange til kommunes netværk via VPN-forbindelser.

Et andet afgørende sikkerhedsmæssigt tiltag har været at sikre, at kommunens pc'er er tilstrækkeligt sikkerhedsopdateret. I forbindelse med covid-19 har Københavns Kommune dels sikret, at sikkerhedsopdateringer gennemføres, når brugeren af pc'en tilgår kommunens it-infrastruktur gennem VPN-forbindelse, og dels gennemført tiltag der muliggør, at der kan hentes sikkerhedsopdateringer fra medarbejdernes egne internetforbindelser.

3. Fortsat øget opmærksomhed på phishingsforsøg
Phishingspillet fra Hoxhunt har været i brug i KK siden 2020 og har til formål at øge opmærksomheden på phishingforsøg blandt it-brugere i kommunen. It-brugerne modtager simulerede phishingmails via kommunens mailsystem og modtager resultater, når de opdager og indrapporterer de simulerede phishingforsøg. Omtrent halvdelen af kommunens administrative medarbejdere deltager i spillet.

I løbet af 2021 er der udviklet nye og tidssvarende udgaver af de simulerede phishingmails og aktuelle trusler, der fortsat øger opmærksomheden på phishingtrusler hos kommunens it-brugere. I september 2021 foretog Økonomiforvaltningen en evaluering af spillet i alle forvaltninger med gode resultater. 94 procent af de adspurgte tilkendegav, at Hoxhunt er en god måde at lære om cybersikkerhed på, og 80 procent mente, at de havde lært noget nyt af at tage del i spillet.

4. Øget kontrol med tildeling af brugerrettigheder
Københavns Kommune gør brug af en såkaldt IGA-platform til styring og kontrol med brugerrettigheder i kommunens it-systemer. Styring med brugerrettigheder skal sikre, at medarbejdere i kommunen kun har den fornødne adgang til data, og at denne adgang lukkes ved ansættelsens ophør.

I forbindelse med idriftsættelsen af IGA-platformen er der i 2021 etableret automatiske oprettelser og nedlæggelser af it-brugere, som er

koblet til kommunens HR-processer. Det betyder, at der oprettes en it-bruger, når en medarbejder ansættes i Københavns Kommune, og den nedlægges igen, når medarbejderen fratræder. Platformen giver derfor en markant bedre beskyttelse af adgangen til de data, som gemmes i kommunens mange it-systemer sammenlignet med manuel styring, da det sikres, at en medarbejder ikke kan have adgang til data efter ansættelsesforholdets ophør.

Samtidig giver IGA-platformen et brugervenligt overblik over aktive it-brugere for både ledere og deres stedfortrædere. Det giver et markant lettere ledelsestilsyn med it-brugere på alle niveauer i organisationen, da platformen kan identificere og overvåge adgange, der konflikter med kommunens regler for økonomistyring. Denne funktion sikrer kommunen bedre mod svindel og underslæb i kommunens økonomibærende systemer.

5. Styrket ledelsesstyring og organisering af informationssikkerheden
Som resultat af den eksterne revision af Københavns Kommunes generelle it-kontroller i 2021 har Økonomiforvaltningen igangsat to initiativer. Formålet med initiativerne er at styrke ledelsessystemet for informationssikkerhed og sikre en tydeligere rolle- og ansvarsfordeling i styringen heraf.

Formålet med indsatserne er at sikre bedre rapportering på informationssikkerhedsområdet samt en dokumenteret vurdering af behov for it-kontroller, en såkaldt SoA (Statement of Applicability). Det vil i den forbindelse blive undersøgt, hvorvidt der kan etableres en fælles it-platform, som kan understøtte arbejdet med den ledelsesmæssige og daglige styring af informationssikkerheden i Københavns Kommune i et såkaldt ISMS-system (Information Security Management System).

De to initiativer må forventes at give anledning til ændringer i Københavns Kommunes eksisterende regelsæt og vil blive gennemført med inddragelse af kommunens kreds af ansvarlige it-direktører.

<u>Databeskyttelsesindsatser i Københavns Kommune</u>
Databeskyttelsesrådgiveren udarbejder hvert år en statusrapport for databeskyttelsesindsatsen i Københavns Kommune. Databeskyttelsesrådgiveren forelagde denne rapport for Økonomiudvalget i begyndelsen af 2022. I rapporten identificerer databeskyttelsesrådgiveren seks særlige risikoområder, der anbefales prioriteret i 2022. Databeskyttelsesrådgiveren vurderer, at Københavns Kommune ved at følge de anbefalingerne, kan opnå et nødvendigt og højere complianceniveau på databeskyttelsesområdet.

På den baggrund har Økonomiforvaltningen i koordination med databeskyttelsesrådgiveren udarbejdet en handleplan for indsatser på

databeskyttelsesområdet. Handleplanen har til formål at løse de risikoområder, som databeskyttelsesrådgiveren har identificeret. For at sikre løsninger der understøtter forvaltningernes behov og sikre ensartet implementering, forankres indsatserne i handleplanen i Københavns Kommunes tværgående GDPR Forum, som blev etableret i 2021 med det formål at styrke en effektiv efterlevelse af reglerne om databeskyttelse i Københavns Kommune.

Som en del af handleplanen har Økonomiforvaltningen i samarbejde med kommunens fagforvaltninger og databeskyttelsesrådgiveren igangsat udvikling og afprøvning af et nyt koncept for risikovurderinger og konsekvensanalyser. Inden udgangen af 2022 forventes konceptet godkendt og implementeret i kommunen i form af nye forretningsgange på området. Økonomiforvaltningens handleplan blev forelagt Økonomiudvalget sammen med databeskyttelsesrådgiverens statusrapport.

Konklusioner fra informationssikkerhedstilsyn og risikovurdering 2021
Koncern IT fører årligt tilsyn med informationssikkerheden i forvaltningerne og gennemfører risikovurderinger af kommunens it-systemer i samarbejde med forvaltningerne. Resultatet af informationssikkerhedstilsynet og risikovurderingerne giver forvaltningerne mulighed for at træffe beslutning om sikkerhedsniveauet inden for egen forvaltning, som det følger af forretningscirkulæret for organisering af informationssikkerhed.

Tilsynet med informationssikkerheden i Københavns Kommune har generelt fundet:

a) at der er behov for mere ensartet dokumentationen af forhold, der skal sikre et tilstrækkeligt informationssikkerhedsniveau i kommunens fælles informationssystem til dokumentation af it-systemer.
b) at der udvalgte steder er behov for udarbejdelse af forvaltningsspecifikke arbejdsgange på informationssikkerhedsområdet.
c) at man bør sikre et generelt højt niveau for forvaltningernes styring og vedligeholdelse af beredskabsplaner for kritiske systemer, herunder tilstrækkeligt grundlag for nødplaner, som klart anviser, hvorledes forretningen skal gennemføre konkrete forretningsprocesser ved systemnedbrud.

Risikovurderingen af kommunens it-systemer viser, at der stedvist er behov for en styrket indsats på informationssikkerhedsområderne for:

a) Procedurer og rolle- og opgavefordeling. Der er behov for bedre styring af autorisationer på en delmængde af

kommunens it-systemer, herunder bedre processer for gennemgang af logs for at analysere uregelmæssigheder.

b) Leverandørstyring. I en delmængde af kommunens it-systemer mangler man dokumentation for målene for tilstrækkelig leverandørdrift og -service i kontrakten.
c) Sårbarhedsstyring. En delmængde af de it-systemer, der gennemfører tests (herunder penetrationstests), som identificerer sårbarheder i it-systemer, bør dokumentere processen.
d) Nedbrud og backup. Der gennemføres ikke i tilstrækkelig grad tests af forvaltningernes it-beredskabsplaner.

Forvaltningerne skal på baggrund af informationssikkerhedstilsynet og risikovurderingen af it-systemer vurdere, om og hvordan der bør ske implementering af tiltag for at sikre et tilstrækkeligt informationssikkerhedsniveau.

Kommunens forvaltninger har på baggrund af risikovurderingerne udarbejdet handleplaner, der er godkendt af forvaltningernes direktion. Kommunens kreds af it-ansvarlige direktører orienteres løbende i It-kredsen om status på implementeringen af disse. Forvaltningerne anbefales ligeledes på baggrund af informationssikkerhedstilsynet at udarbejde forvaltningsspecifikke handleplaner.

Dispensationer fra reglerne for informationssikkerhed

Der er i 2021 blevet udstedt tre nye dispensationer fra kommunens regler for informationssikkerhed. To vedrørende it-systemer tilhørende Beskæftigelse- og Integrationsforvaltningen og én vedrørende it-system tilhørende Sundhedsforvaltningen. Da det ene it-system tilhørende Beskæftigelses- og Integrationsforvaltningen ikke længere anvendes i Københavns Kommune er denne dispensation ikke længere aktuel. For de to øvrige dispensationer gælder, at disse er tidsbegrænsede og betingede af, at der indføres mitigerende foranstaltninger.

Derudover er to dispensationer forlænget vedr. it-systemer tilhørende hhv. Børne- og Ungdomsforvaltningen og Beskæftigelse- og Integrationsforvaltningen. Begge dispensationer er tidsbegrænsede og betingede af, at der indføres mitigerende foranstaltninger. Alle dispensationer er forelagt It-kredsen til orientering.

Informationssikkerhedshændelser 2021

En informationssikkerhedshændelse er en samlebetegnelse for alle typer af hændelser, der kan udgøre en risiko for de informationer, som Københavns Kommune behandler, og som indikerer et muligt brud på informationssikkerheden, herunder tab af data, uautoriseret adgang, videregivelse af data mv. Indebærer informationssikkerhedshændelsen ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, er der tale om et brud på persondatasikkerheden. Hvis et brud på persondatasikkerheden medfører en

sandsynlig risiko for fysiske personers rettigheder eller frihedsrettigheder, skal bruddet anmeldes til Datatilsynet.

Tabel 1: Antal brud på persondatasikkerheden i 2019, 2020 og 2021

	2019	2020	2021
Registrerede persondatasikkerhedsbrud	283	391	344
Anmeldte brud til Datatilsynet	179	179	136

Antallet af brud på persondatasikkerheden i Københavns Kommune ligger på et stabilt niveau. At andelen af indmeldte brud til Datatilsynet er faldende, kan ses som et udtryk for, at forvaltningerne med tiden er blevet bedre til at vurdere, hvornår anmeldelse er nødvendigt.

Tabel 2: Antal it-sikkerhedshændelser i 2019, 2020 og 2021

	2019	2020	2021
It-sikkerhedshændelser	87	124	77

En it-sikkerhedshændelse kan defineres som en informationssikkerhedshændelse, der ikke involverer personoplysninger, men som indikerer et muligt brud på informationssikkerhedspolitikken eller svigt af en kontrol. Antallet af it-sikkerhedshændelser ligger stabilt sammenlignet med 2019. I forhold til 2020 er antallet faldet. Årsagen hertil kan være, at antallet af it-sikkerhedshændelser i 2020 steg midlertidigt pga. mange hjemmearbejdende medarbejdere under pandemien.

Økonomi
Sagen har ikke økonomiske konsekvenser.

Videre proces
Økonomiforvaltningen arbejder videre med de beskrevne tiltag og forelægger Økonomiudvalget en ny status på informationssikkerheden første kvartal 2023.

Bilag

-