KIT Sikkerhed (3447)
Økonomiforvaltningen

Orienteringssag

Til Økonomiudvalget (ØU)

Status for informationssikkerhedsområdet i Københavns Kommune 2023

03-04-2024

Sagsnummer i F2
2023 - 17305

Dokumentnummer i F2
4916439

Sagsnummer eDoc
2023-0404275

Sagsbehandler
Stubbe Wissing

Resumé
Til ØUs orientering forelægges den årligt tilbagevendende status på informationssikkerheden i Københavns Kommune (KK). Med udgangspunkt i den nuværende indsats og de besluttede indsatsområder for 2024 og frem er det Økonomiforvaltningens (ØKF) vurdering, at kommunen har et acceptabelt beskyttelsesniveau for kommunens it-systemer og underliggende it-infrastruktur.

Problemstilling
Indsatsen på informationssikkerhedsområdet planlægges ud fra en risikobaseret tilgang, hvor der foretages en afvejning mellem sikkerhedsmæssige risici og kommunens behov for effektiv og god IT-drift samt borgerservice.

KK arbejder strategisk og operationelt med den risikobaserede tilgang for at sikre, at enhver håndtering af personoplysninger og værdioplysninger i KK sker på en betryggende og tillidsvækkende måde i forhold til kommunens borgere og virksomheder, og at kommunen følger gældende databeskyttelsesregler for behandling af personoplysninger.

Arbejdet med informationssikkerheden som helhed tager afsæt i de lovgivningsmæssige rammer, en vurdering af cybertruslen mod KK samt de årlige tilsyn med informationssikkerheden og risikovurderinger af it-systemer og behandlingsaktiviteter. Ekstern Revision fører desuden tilsyn med de generelle it-kontroller i KK, som en del af den lovpligtige revision.

I takt med den øgede digitalisering er der stigende nationale og europæiske krav til informationssikkerhedsniveauet (se bl.a. NIS2 direktivet nedenfor). Hvis KK fremadrettet skal kunne opretholde niveauet og levere på nye krav og trusler, er der behov for øget finansiering til området.

Løsning
Det overordnede billede af status på informationssikkerheden i KK er gengivet nedenfor med en uddybning i bilag 1.

Cybertruslen

Cybertruslen mod KK var i 2023 fortsat meget høj og følger samme alvorlige trend, som er set over de seneste år. På trods af den stigende trussel fra cyberkriminelle har Koncern IT i 2023 håndteret alle alvorlige angreb, der ville have medført større driftsmæssige konsekvenser.

Initiativer til sikring af informationssikkerheden

ØKF har i samarbejde med kommunens øvrige forvaltninger igangsat fire nye initiativer til sikring af informationssikkerheden i 2023. Det drejer sig om følgende initiativer:

1. *Fortsat sikring af cyberforsvaret* gennem bl.a. bedre beskyttelse mod overbelastningsangreb og et mere restriktivt regelsæt for, hvilken ekstern netværkstrafik, der kan tilgå kommunens netværk. Koncern IT blokerer fortsat dagligt omfattende scanninger fra bl.a. russiske ip-adresser. Det er vurderingen, at det nuværende foranstaltningsniveau er passende.
2. *Etablering af et Cyber- og Informationssikkerhedsprogram*, som skal sikre, at KK kan leve op til de kommende lovkrav i EU's net- og informationssikkerhedsdirektiv (NIS2). Direktivet træder i kraft den 17. oktober 2024 med forsinket implementering i dansk lovgivning (forventet ultimo 2024). Kravene i NIS2 er endnu ikke præciseret for kommunalt niveau, men forventes som minimum at omfatte væsentlige dele af it-infrastruktur, teknik- og miljøområdet samt sundhedsområdet. Manglende overholdelse af NIS2-lovgivningen vil forventeligt kunne medføre sanktioner i form af bøder. Som følge af NIS2 samt en ekstern revisionsbemærkning om behov for styrket ledelsessystem (ISMS) skærpes kravene til styring, organisering og dokumentation på informationssikkerhedsområdet. I 2023 er forarbejdet og de nødvendige indsatser blevet identificeret med henblik på implementering fra 2024.
3. *To nye koncepter for hhv. risikovurderinger af behandlingsaktiviteter og it-systemer* er afprøvet og implementeres hhv. primo 2024 og medio 2024. Formålet er at øge kvaliteten i risikovurderingerne.
4. *Databeskyttelsesindsatser*
    - It-leverandørers brug af KK-personoplysninger til egne formål er en national og europæisk udfordring, idet hjemmelgrundaget ikke er på plads. KK kan ikke selv løse denne udfordring, men arbejder med bedst muligt at tage hånd om udfordringen både i konkrete sager om bl.a. udbud og i dialog med bl.a. KL.
    - Der er fulgt op på Databeskyttelsesrådgiverens statusrapport for 2022, hvor der er arbejdet videre med observationspunkterne om bl.a. en styrket governance på databeskyttelsesområdet. Nogle er videreført til 2023 statusrapporten, som forelægges ØU særskilt. Af denne fremgår også tre særlige risikoområder, der anbefales prioriteret i 2024: Oplysningspligt, uddannelse af medarbejdere i it-sikkerhed og databeskyttelse, og tv-overvågning.

Tilsyn med informationssikkerhed 2023
KIT har gennemført tilsyn på følgende fire områder: 1) Brug af sociale medier, 2) Eksterne konsulenters fjernadgang til administrative it-systemer og servere, 3) Softwareopdatering (Patching) og 4) Udfasning af it-systemer.

Øvrige fokuspunkter
Af vedlagte bilag fremgår desuden information om de årlige it-risikovurderinger, overblik over dispensationer fra reglerne for informationssikkerhed, overblik over informationssikkerhedshændelser 2023 samt tilgangen til it-beredskabet i KK.

Økonomi
Sagen har ikke økonomiske konsekvenser.

Videre proces
Økonomiforvaltningen arbejder videre med de beskrevne tiltag i 2024.

Såfremt Økonomiudvalget ønsker en temadrøftelse om cybersikkerhed, foreslår Økonomiforvaltningen, at den afholdes i efteråret 2024.

Bilag
Bilag 1. Status for informationssikkerheden i Københavns Kommune 2023 – uddybende orientering

KIT Sikkerhed (3447)
Økonomiforvaltningen

Bilag

Til Økonomiudvalget

Status for informationssikkerhedsområdet i Københavns Kommune 2023 – uddybende orientering

28-02-2024

Sagsnummer i F2
2023 - 17305

Dokumentnummer i F2
4916439

Sagsnummer eDoc
2023-0404275

Sagsbehandler
Stubbe Wissing

Resumé
I notatet fremlægges en uddybende orientering om status for informationssikkerheden i Københavns Kommune.

Sagsfremstilling
Trusselsvurdering
Koncern IT opdaterer årligt vurderingen af cybertruslen mod Københavns Kommune og orienterer IT-kredsen. Vurderingen er udgangspunkt for flere indsatser i kommunen, hvor den indgår i grundlaget for de årlige risikovurderinger af it-systemer, som prioriteringsgrundlag for beslutninger om sikkerhedsniveauet i KK's IT-infrastruktur og som prioriteringsgrundlag for beslutninger om sikkerhedsniveauet på cyberområdet.

Cybertruslen mod Københavns Kommune var i 2023 fortsat meget høj og følger samme alvorlige trend, som er set over de seneste år. Siden sidste års vurdering har cybertruslen været særligt centreret omkring nedenstående:

1. Angreb mod it-infrastrukturen
Cyberkriminelle forsøger at finde og udnytte sårbarheder i kommunens it-infrastruktur. Ved at scanne efter udsatte systemer og komponenter forsøger cyberkriminelle at hacke sig til adgang til it-infrastrukturen for efterfølgende at placere ondsindet eller ødelæggende kode i systemer og på netværk.

2. Angreb med mere sofistikerede metoder og teknikker
Både kriminelle og statsstøttede hackere udvikler hele tiden deres metoder og teknikker. Dét, kombineret med den kontinuerlige digitalisering af både den private og offentlige sektor, giver et støt stigende antal potentielle sårbarheder i de mange it-løsninger. Det øger kompleksiteten af det nødvendige cyberforsvar og behovet for hele tiden at følge udviklingen for at sikre sig med de nyeste opdateringer af både styresystemer, programmer og øvrigt software.

3. Ransomware-angreb
Både danske og internationale kilder (private som offentlige) vurderer enslydende, at der ses en fortsat markant stigning i ransomware-

angreb. Danske organisationer og virksomheder bliver ramt dagligt, enten fordi deres systemer ikke er opdaterede, eller fordi en eller flere medarbejdere utilsigtet klikker på links, eller på anden måde får aktiveret ondsindet kode i mails eller fra internettet.

I forhold til sidste års vurdering er der to primære ændringer i det samlede trusselsbillede.

1. Truslen fra både autonome og statsstøttede aktivister er steget fra *middel* til *høj*, idet der ses udbredte DDoS-angreb (overbelastningsangreb) på både statslige organisationer og private selskaber over hele Vesteuropa. CFCS vurderer, at disse angreb med nogen sandsynlighed også kan ramme danske myndigheder.

2. Truslen fra "insidere" er to-delt:

    - Truslen kan komme fra bevidste, ondsindede handlinger udført af ansatte med adgang til KK's IT-systemer. Denne trussel vurderes at være *lav* men stigende. Årsagen er, at der i det seneste år har været eksempler på, at ansatte bevidst har forsøgt at udnytte deres systemadgange til at tilgå data for private relationer/familie, samt et eksempel på, at en ansat har udnyttet kommunens systemer til at begå berigelseskriminalitet.

    - Truslen fra ansatte, som utilsigtet via links i mails, eller andre filer aktiverer ondsindet kode eller bliver snydt til at afgive deres afgangsoplysninger. Ansatte i KK ses også anvende deres KK-brugernavn og adgangskode på en usikker tjeneste på nettet, forsøge at hente usikker software og lignende. Koncern IT ser og forhindrer ofte denne type hændelser, hvorfor risikoen vurderes til fortsat at være høj.

Sammenfatning af trusselsvurderingen
På trods af den stigende trussel fra cyberkriminelle har Koncern IT i 2023 håndteret alvorlige angreb, der ville have medført større konsekvenser for den sikre, forsvarlige it-drift i KK.

<u>Centrale initiativer til sikring af informationssikkerheden 2023</u>
Økonomiforvaltningen har i samarbejde med kommunens øvrige forvaltninger igangsat nye initiativer til sikring af informationssikkerheden i 2023.

1. Fortsat fokus på sikring af cyberforsvar
Den internationale udvikling, herunder krigen i Ukraine, har yderligere skærpet behovet for fokus på cyberområdet.

Center for Cybersikkerhed (CFCS) hævede i 2022 trusselsvurderingen for cyberaktivisme fra lav til *middel* og Økonomiforvaltningen gennemgik ultimo samme år de allerede opsatte foranstaltninger for at optimere kommunens beskyttelse mod overbelastningsangreb. CFCS's vurdering

er for 2023 steget fra *middel* til *høj*, idet der bl.a. ses høj aktivitet fra prorussiske aktivister på cyberområdet. På den baggrund har Københavns Kommune i 2023 opsat et mere restriktivt regelsæt for hvilken ekstern netværkstrafik, der kan tilgå kommunens netværk. Koncern IT blokerer fortsat dagligt omfattende scanninger fra bl.a. russiske, kinesiske og nordkoreanske ip-adresser.

Det er umiddelbart vurderingen, at det nuværende foranstaltningsniveau er passende. Et større overbelastningsangreb kan skabe midlertidige driftsforstyrrelser på kommunens internetvendte tjenester, men risikoen for at det vil påvirke den centrale drift af kommunens it-infrastruktur vurderes at være lav.

2. *Etablering af Cyber- og Informationssikkerhedsprogram forud for lovkrav i EU's Net- og Informationssikkerhedsdirektiv (NIS2)*

Københavns Kommune har begyndt et Cyber- og Informationssikkerhedsprogram, som skal sikre at kommunen kan leve op til de kommende lovkrav i EU's net- og informationssikkerhedsdirektiv (NIS2). Direktivet træder i kraft den 17. oktober 2024 med forsinket implementering i dansk lovgivning (forventet ultimo 2024). Kravene i NIS2 er endnu ikke præciseret for kommunalt niveau, men forventes at være omfattende og som minimum at omfatte væsentlige dele af it-infrastruktur, teknik- og miljøområdet samt sundhedsområdet. Manglende overholdelse af NIS2-lovgivningen vil forventeligt kunne medføre sanktioner.

Som følge af NIS2 samt en ekstern revisionsbemærkning om behov for styrket ledelsessystem (ISMS) skærpes kravene til styring, organisering og dokumentation på informationssikkerhedsområdet. I 2023 er forarbejdet og de nødvendige indsatser blevet identificeret med henblik på implementering fra 2024:

1. Implementering af styrket risikobaseret ledelsessystem til informationssikkerhed (ISMS) for Københavns Kommunes kritiske forretningsprocesser.
2. Opbygning af tværgående koncern CISO-organisation (Chief Information Security Officer) til varetagelse af uafhængige tilsyn, risikovurderinger, afrapporteringer og sikring af robust informationssikkerhed, der er i overensstemmelse med lovgivning, standarder og bedste praksis.
3. Anskaffelse af et GRC-system (Governance, Risk & Compliance) til ledelsesoverblik over kommunens forretningskritiske processer med bedst mulig anvendelse af ressourcer. Systemet vil også understøtte risikovurderinger af it-systemer og behandlingsaktiviteter.

3. *Risikovurderinger af it-systemer og behandlingsaktiviteter*

Koncern IT har i 2023 fortsat arbejdet med et nyt koncept til samlet risikovurdering af it-systemer og lovpligtig risikovurdering af kommunens

behandlinger af personoplysninger. Konceptet gennemgik to afprøvninger på henholdsvis tre og fire it-systemer i efteråret 2023. Det er besluttet, at risikovurdering af hhv. it-systemer og behandlingsaktiviteter adskilles mhp. at sikre, at forvaltningerne hurtigst muligt har kunnet risikovurdere kommunens behandlingsaktiviteter jf. artikel 32 i databeskyttelsesforordningen.

Risikovurderingskonceptet for it-systemer i drift forventes implementeret i maj-juni 2024.

Databeskyttelsesretlige opmærksomhedspunkter
Den 10. juli 2023 vedtog EU-kommissionen en ny tilstrækkelighedsafgørelse for overførsler af persondata mellem EU og USA, som betyder, at Schrems II problematikken vurderes løst og overførsel af personoplysninger til USA isoleret set – igen – kan ske lovligt. Det nye overførselsgrundlag løser ikke problematikken vedr. leverandørernes anvendelse af personoplysninger til egne formål, hvilket stadig vurderes at være en væsentlig udfordring.

Kommunens databeskyttelsesrådgiver har orienteret forvaltningerne herom i sin årsrapport for 2023, og konstateret at det er en stor udfordring, som KK kun vanskeligt kan løse alene. Samtidig har databeskyttelsesrådgiveren anbefalet, at KK inden for de næste 2 år sikrer, at alle kommunens databehandlere ikke anvender kommunens personoplysninger til egne formål samt at der igangsættes initiativer, der medvirker til at problemstillingen løses i samarbejde med andre store nationale aktører såsom KL, regionerne og statslige myndigheder mv.

Problematikken med brug af data til egne formål er senest illustreret ved, at Datatilsynet den 30. januar 2024 har givet påbud til 53 kommuner (ikke Københavns Kommune) i sagen om brug af Google Workspace i folkeskolerne, om at bringe behandlingen af personoplysninger i overensstemmelse med reglerne. Afgørelsen vil forventeligt få større og bredere konsekvenser og pålægge KK en omfattende opgave angående evnen til dokumentation af, hvordan persondata behandles i hele værdikæden hos databehandler og dennes underdatabehandler(e).

Databeskyttelsesrådgiverens statusrapport
Databeskyttelsesrådgiveren udarbejder hvert år en statusrapport for databeskyttelsesindsatsen i Københavns Kommune.

Databeskyttelsesrådgiveren forelægger denne rapport for Økonomiudvalget. I rapporten for 2023 identificerer databeskyttelsesrådgiveren tre særlige risikoområder, der anbefales prioriteret i 2024: Oplysningspligt, uddannelse af medarbejdere i it-sikkerhed og databeskyttelse, og tv-overvågning. Anbefalingen om at prioritere disse tre områder er rettet til alle forvaltninger med henblik på et højere complianceniveau på databeskyttelsesområdet.

I databeskyttelsesrådgiverens statusrapport for perioden 1. oktober 2021 til 1. oktober 2022 indgik anbefalinger til forvaltningerne om at styrke Governance og fremdrift på databeskyttelsesområdet. Med henblik på at imødekomme anbefalingerne, udarbejdede ØKF i 2023 en handleplan med aktiviteter til at styrke koordination, fremdrift og kvalitet i databeskyttelsesindsatsen i KK. Der er på den baggrund udarbejdet en række dokumenter. Det er databeskyttelsesrådgiverende vurdering, at såfremt de dokumenter implementeres som forventet i praksis, vil anbefalingen om en forbedret governance være opfyldt.

Databeskyttelsesrådgiveren har endvidere i sin rapport påpeget vigtigheden af at få gennemført risikovurderinger af behandlinger af personoplysninger.

Årligt tilsyn med informationssikkerhed 2023
Tilsyn med informationssikkerheden i 2023 har haft følgende observationer i forbindelse med årets fire tilsynsemner:

Brug af sociale medier i Københavns Kommune: Anbefaling om en opdateret vejledning for, hvordan informationssikkerhed iagttages ved anvendelse af sociale medier i kommunen.

Eksterne konsulenters fjernadgang: Anbefaling om at sikre tilsyn på it-systemniveau, når eksterne konsulenter har privilegerede rettigheder på KK it-systemer og infrastruktur.

Softwareopdatering: Anbefaling om etablering af en proces for opfølgning hos leverandør for at sikre, at opdateringer til licens/abonnementssoftware og tredjepartskomponenter er identificeret og opdateres løbende af teknisk systemejer.

Udfasning af it-systemer: Anbefaling om, at forvaltningerne følger op på arbejdet med udfasning af it-systemer og sikrer, at arbejdet dokumenteres.

Konklusioner fra de årlige it-risikovurderinger 2023
De årlige risikovurderinger blev gennemført i efteråret 2023. Der blev foretaget risikovurderinger af ét system for hver forvaltning. Risikovurderingerne resulterede i fem handleplaner med i alt 21 handleplanspunkter.

Dispensationer fra reglerne for informationssikkerhed
Siden 2022 har Koncern IT haft fokus på opfølgning og oprydning i dispensationssager. Det øgede fokus har betydet, at der i 2023 er lukket 18 dispensationer. Det betyder, at Københavns Kommune ultimo 2023 havde to igangværende dispensationer: Beskæftigelse- og integrationsforvaltningen (BIF) og Børne- og Ungdomsforvaltningen (BUF) havde hver én dispensation.

Informationssikkerhedshændelser 2023
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.

It-sikkerhedshændelser
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. Tabel 1 viser udviklingen i antallet af it-sikkerhedshændelser de seneste år.

Hvor der de foregående år har været en lettere nedadgående trend i forhold til antallet af indberetninger, er der fra 2022 til 2023 sket en stigning. En årsag til stigningen kan være, at Koncern It i 2023 har forenklet måden at indberette informationssikkerhedshændelser.

Tabel 1: Antal it-sikkerhedshændelser i 2019 - 2023

	2019	2020	2021	2022	2023
It-sikkerhedshændelser	87	124	77	66	95

Persondatabrud 2023
Indebærer en informationssikkerhedshændelse 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 2 viser udviklingen i antallet af persondatabrud de seneste år. I 2023 er der sket en mindre stigning i antallet af registrerede og anmeldte brud, men den generelle trend ses at være stabil.

Tabel 2: Antal brud på persondatasikkerheden 2019 - 2023

	2019	2020	2021	2022	2023
Registrerede brud på persondatasikkerheden	283	391	344	373	399*
Anmeldte brud til Datatilsynet	179	179	136	158	155*

* Tallet viser antal sager, som var afsluttet i kommunens interne sagsbehandlingssystem i perioden 1.1.2023-5.12.2023.

It-beredskab

Reetableringsplaner

En reetableringsplan beskriver, hvordan man bringer et system tilbage i normal drift efter et nedbrud. Planen indeholder oplysninger om leverandør, eventuel sammenhæng med andre komponenter, driftsforhold, sikkerhedskopier, nøglepersoner og vigtige kontaktpersoner, mv.

Koncern It står for drift af infrastruktur for alle kommunens forvaltninger, og har igen i år rettet fokus på reetableringsplaner og deres vedligehold og at de er retvisende. Konkret er der udarbejdet opdaterede planer for reetablering af de væsentligste komponenter i den it-infrastruktur, som Koncern IT har ansvar for, og som forvaltningernes it-systemer er afhængige af.

It-beredskabsøvelse

Koncern It holder hvert år en it-beredskabsøvelse for at teste kommunens it-kriseorganisation, planer mv. i virkelighedsnære nødscenarier. I år havde øvelsen en mere teknisk karakter. Øvelsen blev holdt i september for at teste, om de opsatte sikringsmekanismer var tidssvarende og kunne opdage hackerangreb mod IT-infrastrukturen. Alle angreb blev enten logget eller standset i KK's cyberforsvar og øvelsen gav god viden til at forbedre forsvaret yderligere.