KIT Sikkerhed 2 (5953)
Økonomiforvaltningen

Orienteringssag

Til Økonomiudvalget

Status for informationssikkerhedsområdet 2022

10-03-2023

Sagsnummer i F2
2022 - 19615

Dokumentnummer i F2
2435569

Sagsnummer eDoc
2022-0401342

Sagsbehandler
Tobias Aarsø Larsen
Stubbe Wissing

Resumé
Økonomiforvaltningen orienterer Økonomiudvalget om status på informationssikkerhedsarbejdet, dispensationer fra Københavns Kommunes informationssikkerhedsregler og informationssikkerhedsbrud i kommunen mindst én gang årligt. I 2022 er der gennemført en række indsatser, der imødegår truslerne mod kommunens generelle drifts- og datasikkerhed. Med udgangspunkt i den nuværende indsats og de besluttede indsatsområder for 2023 og frem er det Økonomiforvaltningens vurdering, at kommunens beskyttelsesniveau for kommunens it-systemer og underliggende it-infrastruktur har et acceptabelt niveau. Sagen forelægges til orientering.

Problemstilling
Arbejdet med at sikre en høj informationssikkerhed tager afsæt i en årlig trusselsvurdering, som Økonomiforvaltningen foretager, samt i konklusionerne fra de tilsynsaktiviteter og risikovurderinger, som databeskyttelsesrådgiveren og Økonomiforvaltningen gennemfører årligt. Ekstern Revision fører desuden tilsyn af de generelle it-kontroller i Københavns Kommune som en del af den lovpligtige revision.

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.

Løsning
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.

Trusselsvurdering

Økonomiforvaltningen opdaterer kommunens trusselsvurdering på cyberområdet én gang årligt og orienterer IT-kredsen herom. Overordnet anvendes vurderingen som udgangspunkt for flere indsatser i Københavns Kommune. Vurderingen indgår således både i grundlaget for de årlige risikovurderinger af it-systemer, som prioriteringsgrundlag for beslutninger om sikkerhedsniveauet i Københavns Kommunes it-infrastruktur og som prioriteringsgrundlag for beslutninger om sikkerhedsniveauet på cyberområdet.

Cybertruslen mod Københavns Kommune var i 2022 fortsat meget høj. Internationalt har 2022 været præget af en stigning i antallet af angreb, som også i Københavns Kommune har krævet et stort fokus på cyberforsvaret. I 2022 har der været særligt fokus på tre trusselstyper.

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 tiltvinge sig adgang til it-infrastrukturen for efterfølgende at placere ondsindet og ødelæggende kode i systemer og på netværk. Systemer kan have sårbarheder, der gør dem udsatte uden at producenten er vidende om det (0-dags sårbarhed) eller de kan være udsatte, fordi de ikke er opdateret (patchet) efter producentens anbefalinger.

2. Angreb mod brugere (phishing)
Den hyppigst forekommende type af angreb er rettet mod dét, der ofte omtales som det svageste led i cyberforsvaret, nemlig brugerne. Cyberkriminelles fortrukne angrebsvinkel er via e-mail. Ved at sende en ondsindet e-mail til ansatte i Københavns Kommune, forsøger cyberkriminelle at lokke medarbejdere til at klikke på et link eller åbne en vedhæftet fil. Formålet for de cyberkriminelle er som oftest berigelseskriminalitet, hvor den cyberkriminelle forsøger at afpresse penge fra medarbejdere. Der ses også flere phishingmails, hvor cyberkriminelle forsøger at få medarbejdere til at afsløre deres adgangskoder eller forsøger at placere skadelig kode på deres computer, for derefter at skaffe sig adgang til følsomme oplysninger eller tiltvinge sig yderligere adgang til kommunens it-infrastruktur.

Københavns Kommune oplever dagligt sådanne angreb rettet mod medarbejdere og ser en stadig mere sofistikeret udformning af phishing e-mails. I 2022 er der også observeret mere målrettede phishing e-mails, hvor ondsindede cyberkriminelle har kompromitteret en af kommunens samarbejdspartnere, for derefter at inficere en igangværende mailkorrespondance med skadelige links og indhold.

3. Overbelastningsangreb (DDos-angreb)
Et overbelastningsangreb bliver ofte omtalt som et DDos-angreb og er en angrebstype, hvormed en ondsindet aktør forsøger at sende store mængder internettrafik mod et specifikt mål. Formålet er at overbelaste målet, fx en hjemmeside med så meget trafik, at hjemmesiden ikke har kapacitet til at håndtere al trafikken og dermed bliver utilgængelig. I 2022 er overbelastningsangreb blevet mere tilgængelige for

ondsindede aktører og kan let købes som en service på det mørke net. Cyberaktivister benytter overbelastningsangreb for at fremme omtale af deres egen politiske agenda samt genere deres mål for angrebet. Særligt invasionen af Ukraine har medvirket til en stor stigning af denne type angreb fra pro-russiske grupperinger. Bl.a. på den baggrund har Center for Cybersikkerhed under Forsvaret hævet trusselsvurderingen for cyberaktivisme til niveauet *høj*.

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

1) Risikoen for datalæk som følge af ransomware-angreb vurderes som *meget høj og stigende*
2) Statsstøttet aktivisme er tilføjet som en trusselsaktør forbundet med middel risiko.

Risikoen for utilsigtede datalæk vurderes til fortsat at være høj. Koncern IT ser og forhindrer ofte hændelser, hvor medarbejdere i Københavns Kommune ubevidst har aktiveret et ondsindet link, brugt deres KK-brugernavn og adgangskode på en usikker tjeneste på nettet, hentet usikker software og lignende. Derimod vurderes risikoen fra bevidst ondsindede forsøg på kriminalitet, eller datatyveri fra "insidere" i Københavns Kommune til at være lav.

Sammenfatning

På trods af den stigende trussel fra cyberkriminelle har der i 2022 ikke været kendte angreb, der har haft større konsekvenser for kommunens forsvarlige it-drift.

Centrale initiativer til sikring af informationssikkerheden 2022

Økonomiforvaltningen har i samarbejde med kommunens øvrige forvaltninger igangsat og implementeret en række initiativer til sikring af informationssikkerheden i 2022.

1. Cyberforsvar

Kommunens monitorering af den eksterne netværkstrafik har vist en øget aktivitet fra ikke allierede lande. Dette skal ses i lyset af den eskalerede konflikt i Ukraine, hvor cyberaktivister i højere grad afsøger sårbarheder ved at scanne netværk hos de større myndigheder i EU-landene.

På den baggrund har Københavns Kommune opsat et mere restriktivt regelsæt for hvilken ekstern netværkstrafik, der tillades til kommunens netværk. Ultimo fjerde kvartal 2022 blev der registreret flere målrettede overbelastningsangreb mod danske interesser, herunder ministerier, styrelser og især banker. Økonomiforvaltningen har på den baggrund gennemgået de allerede opsatte foranstaltninger for at optimere kommunens beskyttelse mod overbelastningsangreb. Det er umiddelbart vurderingen, at det nuværende niveau 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 ses at være på et lavere niveau.

2. Udfasning af tidligere brugerstyringsplatform
Med udgangen af 2022 har Økonomiforvaltningen lukket den gamle brugerstyringsplatform, og alle potentielle systemer er omlagt til en ny platform. Den nye platform giver en systematisk styring af hvilke adgange til data, den enkelte medarbejder har. Med omlægningen får personaleledere et bedre samlet overblik over deres medarbejderes it-adgange samt lettere mulighed for at tilbagekalde adgange, hvis der ikke længere foreligger et arbejdsmæssigt formål med adgangen.

3. Risikovurderinger og ibrugtagning af nye it-systemer
Økonomiforvaltningen har i anden halvdel af 2022 arbejdet på et nyt koncept for risikovurderinger, som både rummer en risikovurdering på vegne af kommunens borgere som følge af GDPR-lovgivningen, samt en risikovurdering for Københavns Kommunes forretningsoplysninger.

Konceptet er endnu under udvikling og sker i et tæt samarbejde med kommunens databeskyttelsesrådgiver. Konceptet vil blive implementeret i 2023 og vil både blive benyttet ved anskaffelser af nye it-systemer og ved løbende vurderinger af systemer, der er i drift.

I forbindelse med Ekstern Revisions gennemgang af generelle it-kontroller i 2022 modtog Økonomiforvaltningen en rød revisionsbemærkning vedrørende ibrugtagningen af it-systemer i Københavns Kommune, idet der var taget et it-system i brug i en fagforvaltning uden Økonomiforvaltningen havde udstedt en ibrugtagningstilladelse.

På den baggrund har Økonomiforvaltningen iværksat en handleplan med tilslutning fra alle forvaltninger, der skal sikre, at alle it-systemer i kommunen modtager en ibrugtagningstilladelse, inden disse idriftsættes. ØU er tidligere blevet orienteret om sagen.

Som en del af handleplanen har Koncern IT i Økonomiforvaltningen styrket sin organisering og nedsat et nyt team, der skal styrke og revidere anskaffelsesprocessen af nye it-systemer og den løbende risikovurdering af etablerede systemer.

4. *Opmærksomhed på phishingforsøg og awareness om sikker it-brug*
Via phishingspillet fra leverandøren Hoxhunt har Økonomiforvaltningen siden 2020 sat fokus på phishingforsøg. Gennem spillet har kommunens administrative medarbejdere modtaget simulerede phishingmails via kommunens mailsystem.

Efter koordination med kommunens IT-kreds er Økonomiforvaltningen i gang med at sikre anskaffelse af en ny awareness-løsning. Løsningen skal bygge videre på erfaringerne med Hoxhunts anti-phishing elementer og om muligt nå endnu bredere ud på det generelle awareness-område om sikker it-brug, som fortsat er et prioriteret indsatsområde.

Økonomiforvaltningen prioriterer, at den kommende løsning også kan understøtte dé af kommunens medarbejdere, som fortrinsvis benytter

sig af mobile enheder, og at løsningen kan tilpasses individuelle kampagner med øje for målgrupperne og deres specifikke brug af it.

Databeskyttelsesindsatser i Københavns Kommune

1. Indsats som følge af Schrems-II
EU-domstolens Schrems II-dom af 16. juli 2020 har ulovliggjort grundlaget for overførsler af persondata fra EU til USA.

Som Økonomiudvalget tidligere er orienteret om, skal Københavns Kommune som dataansvarlig sikre, at der fortsat er et gyldigt overførselsgrundlag til de af kommunens databehandlere, der behandler personoplysninger i usikre tredjelande.

I koordination med kommunens databeskyttelsesrådgiver har alle forvaltninger i løbet af 2022 arbejdet med vurdering af tredjelandsoverførsler og identificering af it-systemer med tilsigtede overførsler, for hvilke der er udarbejdet exitplaner og igangsat dialog med databehandlere.

Tidspunktet for, hvornår der godkendes et nyt lovligt overførselsgrundlag mellem USA og EU er endnu ikke kendt, men iagttagere forventer, der kommer et nyt overførselsgrundlag i foråret 2023.

2. Databehandleres brug af data til egne formål
Det er et lovkrav, at der er transparens om anvendelse af data, når Københavns Kommune anvender databehandlere, og der foreligger ikke en gyldig behandlingshjemmel for Københavns Kommune til at videregive personoplysninger til databehandlere, som ønsker at anvende data til egne formål eksempelvis produktudvikling eller markedsføring. Kommunens databeskyttelsesrådgiver har desuden orienteret forvaltningerne herom. Der påhviler derfor alle forvaltninger en væsentlig opgave med at sikre dette såvel i forhold til brug af eksisterende databehandlere som i forhold til indgåelse af nye aftaleforhold.

3. Databeskyttelsesrådgiverens statusrapport
Databeskyttelsesrådgiveren (DPO) udarbejder hvert år en statusrapport for databeskyttelsesindsatsen i Københavns Kommune.

Databeskyttelsesrådgiveren forelagde denne rapport for Økonomiudvalget primo 2023. I rapporten identificerer databeskyttelsesrådgiveren tre særlige risikoområder, der anbefales prioriteret i 2023. Databeskyttelsesrådgiveren vurderer, at Københavns Kommune ved at følge anbefalingerne, kan opnå et nødvendigt og højere complianceniveau på databeskyttelsesområdet.

I databeskyttelsesrådgiverens statusrapport for perioden 1. oktober 2021 til 1. oktober 2022 indgår anbefalinger til forvaltningerne om at styrke governance og fremdrift på databeskyttelsesområdet. Med henblik på at imødekomme databeskyttelsesrådgiverens anbefalinger, har

Økonomiforvaltningen udarbejdet en handleplan med aktiviteter, der har fokus på at styrke koordination, fremdrift og kvalitet i databeskyttelsesindsatsen i Københavns Kommune.

Handleplanen indeholder fire initiativer, som samlet set skal sikre ensartethed, forbedre fremdriften på databeskyttelsesområdet og styrke koordinering af indsatser på tværs af forvaltningerne.

Initiativerne omhandler etablering af et fælles KK-årshjul for aktiviteter på GDPR-området, øget fokus på implementering i GDPR-forum, understøttelse og implementering af DPO's modenhedsanalyser og drøftelse i IT-kredsen med DPO om yderligere tiltag for at styrke governancen på databeskyttelsesområdet.

Med de fire initiativer vurderes det, at der kan skabes klarhed over, hvordan databeskyttelsesretlige opgaver løses bedst muligt med fokus på at gøre tingene ensartet, højne kvalitetsniveauet samt løse opgaverne på en mere omkostningseffektiv måde, og dermed sikre fremdrift i forhold til de almindelige driftsopgaver samt god koordinering af indsatser på tværs.

Økonomiudvalget blev orienteret om handleplanen på møde d. 25. januar 2023. Koncern IT i Økonomiforvaltningen skal sikre, at handleplanen implementeres i et tæt samspil med alle forvaltninger.

<u>Styrket ledelsessystem til informationssikkerhed (ISMS)</u>
Af Ekstern Revisions rapport om generelle it-kontroller for 2021 fremgik det, at der på udvalgte områder er behov for en styrkelse af Københavns Kommunes ledelsessystem for informationssikkerhed (ISMS). På den baggrund er der nedsat et projekt tilknyttet en styregruppe i Økonomiforvaltningen, hvor Intern Revision deltager som observatør. Der er ved at blive udarbejdet en GAP-analyse, som forventes færdig i andet kvartal 2023. GAP-analysen skal bidrage til at identificere indsatsområder med udgangspunkt i sikkerhedsstandarden ISO27001, forud for en kommende implementering af et styrket ledelsessystem.

<u>Konklusioner fra informationssikkerhedstilsyn og risikovurdering 2022</u>
Tilsyn med informationssikkerheden i 2022 viser overordnet, at en eller flere forvaltninger skal styrke sin indsats på følgende områder:

a) *Forvaltningernes ledelsestilsyn på informationssikkerhedsområdet*
   En række forvaltninger har behov for at udarbejde handleplaner, som sikrer, at forvaltningerne benytter kommunens brugerstyringsløsning (IGA) til bestilling af brugeradministration og gennemførelse af ledelsestilsyn for systemer, som indeholder person og/eller værdioplysninger.

b) *Organisatoriske nød- og it-beredskabsplaner*

På tværs af forvaltningerne er der en svingende registrering og opdatering af forvaltningernes reetableringsplaner og nødplaner/forretningsplaner i kommunens beredskabssystem C3. Derudover konstateres det, at der er en mangelfuld gennemførelse af tilbagevendende test af forvaltningernes eksisterende reetableringsplaner og nødplaner/forretningsplaner.

c) *Området for uddannelse af systemejere*
En række forvaltninger har ikke tilstrækkelig fokus på, at alle systemejere har gennemført det obligatoriske e-læringskursus for systemejere.

Den årlige risikovurdering af kommunens it-systemer viser, at der stedvist er behov for en styrket indsats på særligt tre informationssikkerhedsområder:

a) Procedurer for rolle- og opgavefordeling
Der er behov for bedre styring af autorisationer på 10 ud af 29 af årets risikovurderede it-systemer. Derudover er der behov for bedre processer for gennemgang af logs for at analysere uregelmæssigheder.

b) Leverandørstyring
I otte ud af 29 af kommunens it-systemer mangler dokumentation for målene for tilstrækkelig leverandørdrift og -service i kontrakten.

c) Nedbrud og backup
Der er ikke i tilstrækkelig grad gennemført tests af forvaltningernes it-beredskabsplaner.

<u>Dispensationer fra reglerne for informationssikkerhed</u>
I 2022 har Økonomiforvaltningen haft fokus på opfølgning og oprydning i dispensationssager. Det øgede fokus har betydet, at der ultimo 2022 er lukket 17 dispensationer. Det betyder, at Københavns Kommune nu har ni igangværende dispensationer.

De ni dispensationer fordeler sig således: Sundheds- og omsorgsforvaltningen har fire dispensationer, Økonomiforvaltningen (Inklusive Koncernservice og Koncern IT) har to dispensationer. Beskæftigelses- og integrationsforvaltningen, Børne- og Ungdomsforvaltningen og Socialforvaltningen har hver én dispensation.

Dispensationerne handler blandt andet om adgangsstyring, brugeradministration, multifaktor-autentifikation og om logning i forretningscirkulære om informationssikkerhed.

<u>Informationssikkerhedshændelser 2022</u>
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 viser udviklingen i antallet af hændelser de seneste år. I 2022 er der sket en mindre stigning i antallet af registrerede og anmeldte brud, men den generelle trend ses at være stabil.

Tabel 1: Antal brud på persondatasikkerheden 2019 - 2022

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

* Tallet viser antal sager, som var afsluttet i kommunens interne sagsbehandlingssystem primo februar 2023.

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 følger en lettere nedadgående trend, hvor 2020 dog ligger noget over det generelle niveau. Årsagen hertil kan være, at antallet af it-sikkerhedshændelser i 2020 steg midlertidigt pga. mange hjemmearbejdende medarbejdere under pandemien.

Tabel 2: Antal it-sikkerhedshændelser i 2019 - 2022

	2019	2020	2021	2022
It-sikkerhedshændelser	87	124	77	66

<u>It-beredskab</u>

Reetableringsplaner

Den væsentligste aktivitet på området for it-beredskabet i 2022 har fokuseret på opdaterede reetableringsplaner. Det skal bl.a. ses på baggrund af, at den globale energikrise har forhøjet risikoen for planlagte strømudfald (brown-outs) og uplanlagte strømudfald (black-outs). På den baggrund har der været et stort fokus på at forberede

genetableringen af kommunens it-systemer efter et eventuelt strømudfald. 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.

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.

It-beredskabsøvelse
Koncern IT holder hvert år en it-beredskabsøvelse for at teste kommunens it-kriseorganisation, planer mv. i virkelighedsnære nødscenarier.

Den 26. oktober 2022 afholdt Koncern IT en planlagt it-kriseøvelse i kulturhuset Pilegården. Deltagerne var Koncern IT´s krisegruppe og en række medarbejdere fra relevante it-områder. Det primære mål med øvelsen var at sætte fokus på reetablering af normal drift under et forhøjet risikoniveau som følge af situationen i Ukraine.

Den efterfølgende evaluering af øvelsen afdækkede et behov for en tæt dialog med fagforvaltningerne (med henblik på en prioritering af de forretningskritiske systemer) og et endnu tættere samarbejde med kommunikationsområdet. På den baggrund vil Koncern IT fremover sikre et tættere samarbejde med alle forvaltningernes digitaliseringschefer og relevante kommunikationsfolk under kriseberedskab.

Økonomi
Sagen har ikke økonomiske konsekvenser.

Videre proces
Økonomiforvaltningen arbejder videre med de beskrevne tiltag i 2023.

Økonomiudvalget vil modtage den næste status på informationssikkerhedsområdet i tredje kvartal af 2023.

Bilag
-