Koncern IT
Økonomiforvaltningen

Bilag

Til Økonomiudvalget

Bilag 2: Uddybende konklusioner fra tilsyn med informationssikkerheden og risikovurderinger 2019

26. februar 2020

Sagsnummer
2020-0026383

Dokumentnummer
2020-0026383-1

Dette bilag er en uddybende gennemgang af hhv:

1. Koncern IT's tværgående tilsyn med informationssikkerheden i forvaltningerne i 2019
2. Koncern IT's risikovurderinger af forvaltningernes it-systemer i forvaltningerne i 2019.

1) Tilsyn med informationssikkerhed 2019

Jf. forretningscirkulæret for organisering af informationssikkerhed fører Koncern IT (KIT) tilsyn med informationssikkerheden i forvaltningerne, hvor der i 2019 er udvalgt i alt fem emner. Udvælgelsen af tilsynsemner har taget afsæt i en risikobaseret tilgang, hvor Koncern IT har vurderet både sandsynligheden og konsekvenserne i tilfælde af manglende overholdelse af informationssikkerhedsbestemmelserne. Som en del af udvælgelseskriterierne er der bl.a. taget udgangspunkt i emner, hvor der i løbet af året er oplevet konkrete uregelmæssigheder.

Tilsynsemnerne er koordineret med databeskyttelsesrådgiveren og den lovpligtige revisor for Københavns Kommune. Tilsynet indeholder en række henstillinger og anbefalinger, hvor anbefalingerne er frivillige at implementere alt efter forvaltningernes risikovillighed, mens henstillingerne er obligatoriske at implementere.

Konklusioner fra tilsynet med informationssikkerheden

Af tabel 1 fremgår tilsynsemnerne for 2019 inklusive det samlede antal henstillinger og anbefalinger, der er givet på tværs af Københavns Kommune. Dernæst følger generelle konklusioner for tilsynsemnerne på tværs af kommunen.

Tabel 1: Overblik over tilsynsemner på tværs af kommunen 2019

Tilsynsemne	Anbefalinger	Henstillinger
Systemejere - udpegning af forretningsmæssig og teknisk ansvarlig	10	9
Ledelsestilsyn med autorisationer	2	16
Leverandørstyring - tavshedspligtserklæringer	3	1
Logopfølgning - udføres der logopfølgning	8	6
Patch af infrastruktur*	2	0
Total	**25**	**32**

Koncern IT
Strategi og Analyse
Borups Allé 177
2400 København NV

EAN-nummer
5798009809056

*Tilsyn kun relevant for Børne- og Ungdomsforvaltning og Økonomiforvaltningen

Med rollen som systemejer for et it-system i kommunen følger en række opgaver, der bl.a. skal sikre lovmedholdelighed og høj informationssikkerhed. I tilsynet er det generelt konstateret, at reglerne for systemejere og funktionsadskillelse bør indskærpes i forvaltningerne gennem udarbejdelse af planer og/eller processer for dette.

Der skal gennemføres ledelsestilsyn med autorisationer for at sikre, at medarbejderne kun har adgang til de data/funktioner, som de har et arbejdsmæssigt behov for. I tilsynet er det generelt konstateret, at der bør udarbejdes og følges processer, der sikrer gennemførelsen af dette ledelsestilsyn. Herudover viser tilsynsresultaterne, at der skal gøres en indsats for at opnå forståelige beskrivelser af rettigheder og rettighedsstrukturer i kommunens it-systemer.

Leverandører kan i engagementet med kommunen få adgang til data, der skal behandles på betryggende vis. For at sikre dette skal der bl.a. underskrives en tavshedspligtserklæring. Tilsynet viser, at der med enkelte undtagelser foreligger tilstrækkelig dokumentation for, at tavshedspligtserklæringerne er indgået.

Logopfølgning skal bl.a. gennemføres for at identificere, hvorvidt brugere har udført handlinger i strid med kommunes regler og lovgivningen. Tilsynet har konstateret, at der er flere it-systemer hos forvaltningerne, hvori der ikke gennemføres logopfølgninger. Der bør derfor gennemføres periodisk logopfølgning på forvaltningernes it-systemer, herunder udarbejdes arbejdsgange, der sikrer opfølgning på logdata.

Regelmæssig opdatering (patch) af infrastruktur minimerer muligheden for, at infrastrukturen bliver angrebet. Tilsynet har konstateret, at der overordnet er en tilstrækkelig beskrivelse af patch-processen af infrastrukturen.

2) Risikovurderinger på systemniveau 2019
I 2019 har KIT foretaget risikovurderinger af 61 it-systemer. Risikovurderingerne indeholder overordnet en række henstillinger og anbefalinger, hvor anbefalingerne er frivillige at implementere alt efter forvaltningernes risikovillighed, mens henstillingerne primært knytter sig til egentlige lovkrav og derfor er obligatoriske at implementere. I 2019 har der været fokus på at risikovurdere systemer indeholdende personoplysninger.
Formålet med risikovurderingerne er at skabe et grundlag for, at ledelsen i de enkelte forvaltninger kan tage stilling til, om de

identificerede risici fra et forretningsmæssigt perspektiv er acceptable, eller om der skal iværksættes yderligere sikringsforanstaltninger.

I en risikovurdering skal antallet af sikringsforanstaltninger afspejle de aktuelle trusler mod et system, og de skal afstemmes ift., hvor kritisk systemet er for forvaltningens fortsatte drift. Valg og fravalg af sikringsforanstaltninger kan således være forskellige fra system til system.

Konklusioner fra it-risikovurderingerne
For hvert af de 61 risikovurderede it-systemer er der taget stilling til tilstedeværelsen af 77 mulige sikringsforanstaltninger fordelt på 12 kontrolområder, jf. tabel 2. Efter tabellen følger en række generelle konklusioner for risikovurderingerne for 2019.

Tabel 2: Oversigt over risikovurderinger på kontrolområder

#	Kontrolområde	Anbefalinger	Henstillinger
1	Fysisk sikring af lokation (perimetersikring) og sikring af adgangspunkter (servere, routere m.v.)	3	0
2	Procedurer og rolle/opgavefordeling for understøttelse af tekniske sikkerhedsforanstaltninger (adgangstildeling, logreview m.v.)	122	0
3	Den registreredes adgang til rettelse/opdatering af registrerede oplysninger	0	107
4	Mobilt udstyr og fjernarbejdspladser	15	0
5	Leverandørforhold	37	0
6	Anskaffelse, udvikling og vedligeholdelse af it-systemer	43	0
7	Sårbarhedsstyring af netværk og kritiske systemer	14	0
8	Kryptering	7	7
9	Logning og overvågning	23	26
10	Nedbrud, backup og disaster recovery	37	10
11	Dokumentation af systemer, herunder versionsstyring og arkitektur	34	0
12	Kommunikationssikkerhed ift. at udstille og hente data	19	0

	Total	**354**	**150**

På tværs af de risikovurderede systemer i kommunen står særligt to kontrolområder frem, som der skal være fokus på i 2020. Det gælder *"den registreredes adgang til rettelse/opdatering af registrerede oplysninger"* og *"procedurer og rolle/opgavefordeling for understøttelse af tekniske sikkerhedsforanstaltninger"*. Begge kontrolområder relaterer sig primært til organisatoriske foranstaltninger, der skal gennemføres for at øge sikkerheden.

Henstillinger
Der er givet 107 henstillinger på kontrolområdet *"den registreredes adgang til rettelse/opdatering af registrerede oplysninger"*, som særligt knytter sig til sletning og opbevaring af data. Udover at der ofte udestår en vurdering af, hvor længe data må opbevares, er det i flere tilfælde konstateret, at der ikke er teknisk mulighed for at slette personoplysninger i systemet.
Herudover er der givet 26 henstillinger til it-systemer i forhold til logning og overvågning. Henstillingerne omhandler særligt etablering og/eller sletning af logs, så det er muligt at etablere et revisionsspor eller udføre andre kontroller i systemet.
10 af de afgivne henstillinger vedrører evnen til at håndtere nedbrud, backup og disaster recovery, hvilket retter sig mod it-beredskabsplanerne it-systemerne.

Anbefalinger
De 122 anbefalinger om *"procedurer og rolle/opgavefordeling for understøttelse af tekniske sikkerhedsforanstaltninger"*, knytter sig særligt til procedurerne og det organisatoriske setup ift. styringen af brugere og adgange. Herudover knytter anbefalingerne sig til procedurerne, der skal sikre systematisk/periodisk logopfølgning, hvilket også var observationen i tilsynet med informationssikkerheden.

Videre proces
Økonomiforvaltningen følger op i It-kredsen på forvaltningernes mitigerende tiltag i forhold til at vurdere kommunens samlede evne til at leve op til informationssikkerhedsbestemmelserne og databeskyttelsesforordningen.