KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncern IT

NOTAT

Til Økonomiudvalget

25. februar 2019

Sagsnr.
2019-0032785

Dokumentnr.
2019-0032785-9

Sagsbehandler
Casper Ranzau Bellincampi

Bilag 5: Uddybende konklusioner på tilsyn med informationssikkerheden 2018

Baggrund

Koncern IT (KIT) fører i henhold til kommunens forretningscirkulærer for organisering af informationssikkerhed årligt tilsyn med overholdelsen af kommunens informationssikkerhedsbestemmelser. Tilsynet skal, jf. Informationssikkerhedsregulativet for Københavns Kommune (KK) foretages ud fra en risikobaseret tilgang, hvor KIT's årlige tilsyn skal bidrage til, at det samlede tilsyn i kommunen er dækkende, tilstrækkeligt og effektivt.

Indledning

KIT har i 2018 udvalgt i alt fem tilsynsemner, som der er ført tilsyn med. De fem tilsynsemner er udvalgt med afsæt i den tilgængelige viden, som KIT er i besiddelse gennem enhedens rolle på informationssikkerhedsområdet i KK. Udvælgelsen af tilsynsemner har taget afsæt i en risikobaseret tilgang, hvor KIT 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.

I 2018 er gennemført tilsyn på følgende tilsynsemner:

A. TV- og videoovervågning
B. Databærende medier
C. Eksterne konsulenters adgange
D. Uddelegeret brugerstyring
E. Sikre kommunikationsløsninger

Tilsynets overordnede formål

Formålet med det gennemførte tilsyn er at lave en vurdering af, hvorvidt forvaltningerne følger kommunens informations-sikkerhedsbestemmelser. Tilsynet skal bidrage til, at forvaltningerne får et indblik i om der er områder, hvor informationssikkerheden ikke er tilrettelagt hensigtsmæssigt og samtidig får anbefalinger til, hvordan informationssikkerheden for de givne emner/områder kan øges.

Nedenfor følger en gennemgang af hvert af de fem tilsynsemner, hvor bestemmelser, formålet og resultaterne for de enkelte tilsynsemner er

Vejledende Sikkerhed

Borups Allé 177
2400 København NV

EAN nummer
5798009809308

uddybet. For alle tilsynspunkter og for tilsynsemnerne generelt anvendes risikobeskrivelsen, der fremgår af Tabel 1 nedenfor.

Tabel 1: Risiko- og prioritetsbeskrivelser

Risikobeskrivelse	Risiko/prioritet
Anvendes for risici, der anses for kritiske. En risiko anses for kritisk, såfremt der er en høj grad af sandsynlighed for, at forholdet indtræffer og/eller har en betydelig effekt og/eller har en betydelig udbredelse.	
Anvendes for risici, der anses for væsentlige. En risiko anses for væsentlig, såfremt der er en middel grad af sandsynlighed for, at forholdet indtræffer og/eller har en vis effekt og/eller har en vis udbredelse.	
Anvendes for risici, der anses for mindre væsentlige. En risiko anses for mindre væsentlig, såfremt der er en lille grad af sandsynlighed for, at forholdet indtræffer og/eller har en lille effekt og/eller har en lille udbredelse.	

A) Tilsyn med forvaltningernes TV- og videoovervågning

Det følger af Københavns Kommunes uddybende it-sikkerhedsregler pkt. 9.3., at forvaltningernes ledelse er ansvarlig for at sikre områder på passende vis. Ledelsen skal endvidere sikre, at tv- og videoovervågning overholder de gældende lovkrav om beskyttelse af persondata samt i øvrigt kommunens egne regler, jf. Københavns Kommunes uddybende it-sikkerhedsregler pkt. 10.10.2.

Formål
Formålet med det udvalgte emne er at undersøge, hvorvidt forvaltningen har et ajourført overblik over hvor der er opsat videoovervågning samt sikret at forvaltningerne overholder en række af Københavns kommunes regler om brug af videoovervågning.

Resultaterne fremgår af Tabel 2 på næste side.

Tabel 2: Resultat for tilsynsemnet: tv- og videoovervågning

Tilsynspunkt	**Status for KK's forvaltninger**		**Risiko og væsentlighed**
	Antal forvaltninger	Opfyldelsesgrad	
Har forvaltning udarbejdet overblik over hvor der er opsat videoovervågning	6	Har nødvendigt overblik	
	1	Har et delvist overblik	
Har forvaltningen informeret udvalgte persongrupper i forbindelse med etablering af videoovervågning	2	Har informeret	
	4	Har informeret delvist	
	1	Har ikke informeret	
Har forvaltning sikret at optagelser gemmes i maksimalt 30 dage samt udarbejdelse instrukser eller vejledninger herfor.	4	Gemmer maksimalt 30 dage	
	2	Har ikke et totalt overblik over området	
	1	Sikrer generelt ikke overholdelse af 30 dages reglen.	
Forvaltningens håndtering af modtagne indsigtsbegæringer efter databeskyttelsesforordningens art. 15	7	Har ikke modtaget anmodning om indsigt i Videooptagelser	
Har forvaltning etableret overvågning af offentlige steder med almindelig færdsel	6	Har registreret overvågning af offentlige steder	
	1	Mangler overblik over karakteren af overvågning	
Har forvaltning etableret skiltning i forbindelse med overvågning	4	Har etableret skiltning	
	1	Har delvist etableret skiltning	
	2	Har ikke et centralt overblik over skiltning	
Har forvaltning indgået aftale med lokale interessenter i forbindelse med etablering af videoovervågning	2	Indgår aftale med lokale interessenter	
	5	Oplyser at der ikke er indgået aftaler med lokale interessenter	
Har forvaltning overblik over hvilke personer som har adgang til videooptagelser	2	Kan dokumentere personer med rettigheder	
	4	Har ikke en central registrering eller mangelfuld registrering	
	1	Har ingen dokumentation om registrerede brugere	

Tilsynets konklusion	Der er væsentlige indikationer på, at forvaltningerne ikke lever op til, eller mangler overblik over, væsentlige dele af de informationssikkerhedsmæssige bestemmelser, der er gældende ift. tv- og videoovervågning. Dette gælder specifikt for: • Sikring af underretning og aftaler med medarbejder samt lokale interessenter. • Overholdelse af sletteregler • Skiltning om videoovervågning • Manglende overblik og registrering af medarbejdere med adgang til videoovervågningsudstyr. Tilsynet har desuden bemærket, at der syntes at være en manglende koordinering af forvaltningernes registreringer lokalt i forhold til det etablerede samarbejde med Københavns Politi.	

B) Tilsyn med databærende medier

- *Procedurer for bortskaffelse af databærende IT-udstyr.*

Ifølge Københavns Kommunes uddybende it-sikkerhedsregler pkt. 9.4.3. følger det, at it-udstyr, som indeholder person- eller værdioplysninger, skal destrueres i det omfang, det er muligt.
Det følger endvidere af kommunens informationssikkerheds regler, at der ikke må opbevares værdi- eller persondata på databærende medier uden den nødvendige beskyttelse.

Formål

Formålet med det udvalgte emne er at undersøge, hvorvidt forvaltningen har retningslinjer for og overblik over anvendelsen samt om der sker en tilbagelevering af databærende medier som f.eks. løse harddiske, USB-nøgler, CD, DVD mv.

Resultaterne fremgår af Tabel 3 på næste side:

Tabel 3: Resultat for tilsynsemnet: databærende medier

Tilsynspunkt	Status for KK's forvaltninger		Risiko og væsentlighed
	Antal forvaltninger	Opfyldelsesgrad	
Udarbejdelse af lokale retningslinjer for benyttelse af databærende medier f.eks. løse harddiske, USB-nøgler, CD, DVD, mobile enheder (tablets, mobiltelefoner)	7	Har ikke modtaget anmærkninger ift. punktet	
Overblik over øvrige databærende medier	7	Har ikke modtaget anmærkninger ift. punktet	
Sikring af tilbagelevering af databærende medier efter medarbejderens ophør eller organisatorisk flytning	7	Har ikke modtaget anmærkninger ift. punktet	
Sikring af sikker destruktion af databærende medier (bortset fra aktiver i Koncern IT's CMDB) samt retningslinjer herom	7	Har ikke modtaget anmærkninger ift. punktet	
Tilsynets konklusion	Tilsynet finder at ingen forvaltninger har overtrådt gældende regler om bortskaffelse af databærende IT-udstyr. I forbindelse med tilsynet har Koncern IT imidlertid henstillet til, at forvaltningerne vurderer, hvorvidt der er behov for yderligere initiativer til at sikre databærende medier. Dette skal bl.a. ske ved, at det bør overvejes om området bør beskrives nærmere.		

C) Tilsyn med eksterne konsulenters adgange

- *Procedurer for eksterne konsulenters adgang til servere mv.*

Det følger af Københavns Kommunes uddybende it-sikkerhedsregler pkt. 10.2., at Københavns Kommune skal kunne gennemføre audit eller kontrol med outsourcede aktiviteter herunder logning af adgang og ændringer til systemer.

Formål
Formålet med det udvalgte emne er at undersøge, hvordan forvaltningerne håndterer de informationssikkerhedsmæssige aspekter, der følger af at samarbejde med eksterne konsulenter. Nærmere har formålet været at undersøge, hvorvidt forvaltningerne har retningslinjer for eksterne konsulenters brugeradgange til servere og systemer som administratorer samt om forvaltning logger (registrerer) og fører tilsyn med konsulenters aktiviteter og rettigheder.

Resultaterne fremgår af Tabel 4 på næste side.

Tabel 4: Resultat for tilsynsemnet: eksterne konsulenters adgange

Tilsynspunkt	**Status for KK's forvaltninger**		**Risiko og væsentlighed**
	Antal forvaltninger	Opfyldelsesgrad	
Retningslinjer for tildeling og sletning af eksterne konsulenters brugeradgange til servere og systemer som systemadministratorer	3	har retningslinjer for tildeling af autorisationer til eksterne konsulenter	
	4	har delvist udarbejdet retningslinjer	
Logning af eksterne konsulenters aktiviteter på de pågældende servere mv.	2	gennemfører logning af konsulenters aktiviteter	
	5	gennemfører kun i begrænset omfang logning af eksterne konsulenter aktiviteter	
Tilsyn med eksterne konsulenters aktiviteter	4	fører tilsyn med eksterne konsulenters aktiviteter	
	2	fører delvist tilsyn eller er i færd med at føre tilsyn med eksterne konsulenter aktiviteter	
	1	fører intet tilsyn med konsulenter	
Tilsyn med sletning af eksterne konsulenters brugeradgange.	5.	fører tilsyn med at eksterne konsulenter slettes efter ophør.	
	2	fører ikke tilsyn med, eller kan ikke dokumentere evt. gennemført tilsyn	
Tilsynets konklusion	Tilsynet finder at der en væsentlig risiko for at manglende retningslinjer, logning og tilsyn med eksterne konsulenter, medfører en forøget risiko for tab af fortrolighed, integritet og tilgængelighed. KIT har på baggrund af tilsynsresultaterne lagt op til en drøftelse heraf i Digitaliseringschefkredsen samt påbegyndt udformningen af en vejledning.		

D) Tilsyn med uddelegeret brugerstyring

- *Procedurer for brugeradministration i systemer som er uddelegeret til lokal styring i forvaltningerne*

Det følger af Københavns Kommunes tidligere it-sikkerhedsregulativ § 7 stk. 4a, at administrationen af brugeradgange i Københavns Kommunes it-systemer varetages af Brugeradministrationen i Koncernservice (nu Koncern IT).

Koncern IT har gennemført en stikprøvekontrol for 5 af de systemer, hvor varetagelsen af brugeradministrationen er uddelegeret til varetagelse lokalt i forvaltningerne.

Formål
Formålet med det udvalgte emne er at undersøge, hvorvidt forvaltningerne har udarbejdet en specifik autorisationsprocedure, der sikrer korrekte procedurer for tildeling og sletning af autorisationer.

Resultaterne fremgår af Tabel 5 nedenfor:

Tabel 5: Resultat for tilsynsemnet: uddelegeret brugerstyring

Tilsynspunkt	**Status for KK's forvaltninger**		**Risiko og væsentlighed**
	Antal forvaltninger	Opfyldelsesgrad	
Autorisationsprocedure for systemet	4	opfylder kravene til autorisationsproceduren	
	1	synes kun at have et delvist billede af autorisationsproceduren	
Sikring af sletning af medarbejdere som ophører eller ikke længere skal have systemadgang.	5	sikrer at medarbejdere slettes ved ophør eller ved bortfald af opgaver.	
Procedure for tildeling af nye adgangskoder i tilfælde af skift af adgangskode.	4	opfylder kravene til en procedure for tildeling af adgangskoder	
	1	giver ikke tilstrækkelig sikkerhed ved adgangskodeskift og passwordkompleksitet	
Tilsynets konklusion	Tilsynet finder at der med de fundne forhold er en mindre risiko for, at de beskrevne autorisationsprocesser ikke er tilstrækkelige. Kvaliteten og udformningen af procedurerne er imidlertid svingende og bygger alene på de centrale regler. Bl.a. i den forbindelse har KIT udarbejdet en vejledning, der skal øge kvaliteten af nuværende og fremtidige autorisationsprocedurer.		

E) Tilsyn med sikre kommunikationsløsninger

- *Borgeres mulighed for at sende sikker e-mail via en række af Københavns kommunes hjemmesider på http://www.kk.dk.*

Det følger af kommunens uddybende it-sikkerhedsregler, navnlig punkt 11.3., at kommunen skal kunne kommunikere sikkert med borgere og virksomheder. Der gælder endvidere et krav om, at

kommunen skal stille løsninger til rådighed, så borgere og virksomheder kan skrive sikkert til kommunen, hvis der skal sendes fortrolige eller følsomme oplysninger over det åbne internet.

Formål
Formålet med tilsynsaktiviteten er at tjekke, hvorvidt der stilles sikre kommunikationsløsninger til rådighed når dette bør være til stede, og at der i øvrigt ikke afgives misvisende informationer omkring kommunikationen. Koncern IT har foretaget en stikprøvekontrol af 50 borgerrettede hjemmesider og de tilknyttede informationer.

Resultaterne fremgår af Tabel 6 nedenfor.

Tabel 6: Resultat for tilsynsemnet: sikre kommunikationsløsninger

Tilsynspunkt	**Status for KK's forvaltninger**		**Risiko og væsentlighed**
	Antal forvaltninger	Opfyldelsesgrad	
Forvaltningens procedurer for borgeres mulighed for at sende sikker e-mail via Københavns Kommune hjemmesider	5	har ikke modtaget nogle bemærkninger for deres håndtering af sikre kommunikations-løsninger.	
	2	har modtaget bemærkninger, fordi det er Koncern IT's vurdering, at der er en betydelig risiko for, at borgere fremsender fortrolige eller følsomme oplysninger ukrypteret til forvaltningernes enheder.	
Tilsynets konklusion	Tilsynet finder, at der generelt er en mindre sandsynlighed for at borgere ikke har mulighed for at sende sikker mail til København Kommunes forvaltninger. Tilsynet peger dog på, at forvaltningerne altid skal sikre, at sider hvor det kan forventes at borgere henvender sig skriftligt, gives mulighed for at sende sikker post.		

Den videre proces
ØKF/Koncern IT foretager løbende tilsyn med overholdelsen af kommunens informationssikkerhedsbestemmelser og kan i den forbindelse bl.a. udstede påbud til forvaltningerne med henblik på, at kommunens regler for informationssikkerhed overholdes, jf. kommunens forretningscirkulære for organisering af informationssikkerhed.

Hertil kommer, at ØKF/Koncern IT bl.a. på baggrund af de respektive tilsyn i forvaltningerne mindst en gang årligt orienterer Økonomiudvalget om status på informationssikkerhedsarbejdet i kommunen, jf. nærværende status.