KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncern IT

NOTAT

25. februar 2019

Sagsnr.
2019-0032785

Dokumentnr.
2019-0032785-8

Sagsbehandler
Casper Ranzau Bellincampi

Bilag 4: Uddybende resultater fra risikovurderinger på systemniveau i 2018

Baggrund

Koncern IT har i 2018 foretaget risikovurderinger i alle forvaltninger af 65 forretningskritiske systemer.

Formålet med risikovurderingerne har været 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.

For hvert af de 65 forretningskritiske systemer er der således taget stilling til tilstedeværelsen af 91 mulige sikringsforanstaltninger fordelt på ti kontrolområder:

- Logning og logreview
- Drifts- og service rutiner
- Leverandørforhold
- Lovmæssige krav
- It-drift og vedligeholdelse
- It-support og brugeradministration
- Dokumentation
- Mobile enheder
- Ledelse og medarbejdere
- Fysisk sikkerhed

Københavns Kommune som helhed

Det er Økonomiforvaltningens umiddelbare vurdering, at forvaltningerne rent systemteknisk på en række parametre lever op til væsentlige it-sikkerhedskrav.

Der ses imidlertid et potentiale i, at forvaltningerne i højere grad tager stilling til it-sikkerhedsmæssige behov på systemniveau. På tværs af kommunen er det særligt logning i systemer, systemorienteret beredskab, systemrettet uddannelse, adgangsstyring og leverandørstyring, hvor der findes det største potentiale.

Økonomiforvaltningen har i tabel 2 nedenfor angivet de hyppigst fraværende foranstaltninger inden for de 65 risikovurderede systemer:

Vejledende Sikkerhed

Borups Allé 177
2400 København NV

EAN nummer
5798009809308

Tabel 1: Hyppigst fraværende foranstaltninger

Kontrolområde	Manglende foranstaltninger som bør overvejes implementeret	Relevant ift. systemer (antal)
Logning & logreview	Manglende automatisk opfølgning på kritiske hændelser i loggen	38
Logning & logreview	Manglende skriftlige/faste procedurer for indsamling og gennemgang af logfiler	37
Logning & logreview	Manglende manuel gennemgang og opfølgning på logfiler	36
Logning & logreview	Manglende skriftlige/faste procedurer for kontrol af logs	36
Drifts- og servicerutiner	Manglende test af beredskabsplan	36
Leverandørstyring	Manglende driftsrapporter fra leverandører	35
Drifts- og servicerutiner	Manglede fastsættelse af driftsmål mv. (RTO og RPO)	31
Leverandørstyring	Manglende servicemål (Service Level Agreement)	29
It-support og brugeradministration	Manglende nedskrevne politik/retningslinjer for adgang til systemer	28
It-drift og vedligeholdelse	Manglende separate udviklings-/testmiljøer til nye funktionaliteter	28
Ledelse og medarbejdere	Manglende formel uddannelse for den konkrete anvendelse af systemet	27
Drifts- og servicerutiner	Manglende gennemførsel af genetablerings tests	27
Drifts- og servicerutiner	Manglende sikring af backup ift. en krypteringsproces	26

Det er Økonomiforvaltningens vurdering, at der på tværs af kommunen særligt bør være fokus på logopfølgning og leverandørstyring. Økonomiforvaltningen vil medio 2019 følge op på forvaltningernes håndtering af de identificerede risici.

Fysisk bygningssikring

En ekstern konsulentvirksomhed har foretaget en analyse af cyber-sikkerheden i KK og er i den forbindelse fremkommet med en række anbefalinger. En af disse anbefalinger knytter sig til etablering af yderligere fysisk sikring af lokationen Fuglebakken, hvor Koncern IT er placeret med kritisk it-infrastruktur. Anbefalingerne indeholder bl.a. en etablering af en central indgangssluse.

Anbefalingen om etablering af fysisk bygningssikring er også inddraget og opretholdt i kommunens samlede risikovurderinger af it-systemer på ØKF's område. Det er i den forbindelse forudsat, at initiativet kan gennemføres i 2019 med henblik på at nedsætte risikoen

for brud på informationssikkerheden. Den yderligere sikring af Fuglebakken drøftes af direktionerne på lokationen.

Den videre proces
ØKF/Koncern IT foretager årligt risikovurderinger af kommunens it-systemer og afgiver i den forbindelse rapporter herom til forvaltningerne, jf. kommunens forretningscirkulære for organisering af informationssikkerhed. På baggrund af risikorapporterne arbejder forvaltningerne videre med implementering af eventuelle yderligere sikringsforanstaltninger. Det er aftalt i it-direktørkredsen, at ØKF i andet kvartal 2019 sikrer, at der sker en opfølgning på forvaltningernes videre arbejde med risikorapporterne.

Hertil kommer, at ØKF/Koncern IT på baggrund af de respektive risikovurderinger har ansvaret for hver andet (lige) år at udarbejde en samlet risikovurdering for kommunen.