



KØBENHAVNS KOMMUNE

Økonomiforvaltningen

Koncern IT

NOTAT

Til Økonomiudvalget

25. februar 2019

Bilag 6: Status på øvrige sikkerhedsområder 2018

Sagsnr.
2019-0032785

Iflg. den fællesoffentlige digitaliseringsstrategi 2016-2020 skal alle offentlige myndigheder følge principperne i den internationalt anerkendte ISO27001-standard for informationssikkerhed. I Københavns Kommune (KK) er principperne udmøntet i 10 sikkerhedsområder, som er defineret nærmere i forretningscirkulæret for informationssikkerhed.

Dokumentnr.
2019-0032785-14

Sagsbehandler
Casper Ranzau Bellincampi

De tre første afsnit i årets status dækker over aktiviteter på 4-5 af de sikkerhedsområder, som der i 2018 har været størst fokus på i KK. Dette bilag giver et overblik over de største og væsentligste initiativer på de øvrige sikkerhedsområder jf. tabel 1 nedenfor:

Vejledende Sikkerhed

Borups Allé 177
2400 København NV

EAN nummer
5798009809308

Tabel 1: Væsentlige initiativer på øvrige sikkerhedsområder i 2018

Informations-sikkerhedsområde	Status
Styring af aktiver	Systemer med persondata er gennemgået i kommunens fortegnelse over systemer, som et led i implementeringen af databeskyttelsesforordningen.
Adgangsstyring	I 2018 er der foretaget en større oprydning af adgange og processer for oprettelse af eksterne konsulenter. I forbindelse med overgangen til Office365 udførte forvaltningerne en oprydning i indholdet og adgange til fællesdrev. Der er i 2019 igangsat et projekt, der skal sikre afklaringen af behovet for yderligere oprydningsaktiviteter.
Driftssikkerhed	KIT overvåger driftsstatus og udefrakommende trusler på centrale dele af it-infrastrukturen. For at forbedre driftssikkerheden er det system, som bl.a. anvendes til at scanne indkomne e-mails for virus/phishing, blevet udskiftet.
Kommunikation og netværkssikkerhed	Der er indført en øget kontrol af netværksudstyr, og der sker løbende udskiftning af forældede platforme. I 2019 påbegyndes implementeringen af en opdeling af kommunens netværk (net-segmentering), og samtidig gennemfører kommunen månedlige penetrationstest for at identificere eventuelle svagheder. Endelig udvides overvågningen af den samlede installation i KIT.
Anskaffelse, udvikling og vedligehold af systemer	Der er i 2018 blevet fastsat nærmere regler for it-anskaffelser. KIT har givet én dispensation fra informationssikkerhedsreglerne i 2018 til Sundheds- og Omsorgsforvaltningen.
Leverandørforhold	I forbindelse med implementeringen af databeskyttelsesforordningen er der indgået et betydeligt antal databehandleraftaler i 2018.
Sikkerheds- og persondatabrud samt beredskabsplaner	Der er i 2018 registreret 120 informationssikkerhedshændelser. Hændelserne er til en vis grad karakteriseret ved at omhandle menneskelige fejl eller forsøg på udnyttelse af fejlene, som f.eks. glemsomhed ved at lukke døre efter sig eller sende mails til forkerte modtagere. Den øgede monitorering af kommunes installationer vil kunne føre til at både menneskelige og tekniske fejl i højere grad identificeres og registreres. I 2018 er der på det tværgående KK-niveau blevet udviklet og godkendt en ny plan for fortsat it-drift samt en strategiske plan for it-genopretning. Forvaltningerne har udarbejdet eller udarbejder pt. lokale it-beredskabsplaner, der skal indgå i styringen af området.

Den videre proces

Som anført i skemaet ovenfor er der iværksat en række initiativer for 2019. I tilknytning hertil bemærkes, at BR ultimo 2018 bevilgede midler til en ekstra it-sikkerhedsindsats på cyber-området, som Koncern IT i 2019 udmønter i en række konkrete initiativer.