KØBENHAVNS KOMMUNE
Koncernservice
Digitalisering

NOTAT

Til ØU

08-12-2014

Sagsnr.
2014-0242420

Dokumentnr.
2014-0242420-2

Sagsbehandler
Irene Ludvigsen

Initiativer til at forbedre It-sikkerheden i Københavns Kommune

Baggrund
Koncernservice orienterede i juni 2014 Økonomiudvalget om status for aktuelle It-sikkerhedsaktiviteter. Det skete på baggrund af den såkaldte IBM/Nets sag, hvor fortrolige data efter oplysninger i medierne blev videregivet af en medarbejder hos IBM til Se & Hør.

Ekstern vurdering
Samtidig anmodede Koncernservice konsulentfirmaet PwC om at analysere sikkerhedsniveauet i Københavns Kommune, dvs. både i Koncernservice og i forvaltningerne.

PwC's rapport er nu modtaget og kan udleveres til Økonomiudvalgets medlemmer ved henvendelse til Borgerrepræsentationens Sekretariat.

PwC vurderer, at Københavns Kommune i dag anvender fornuftige rutiner til styring af It-sikkerheden ud fra et traditionelt trusselsbillede.

Trusselsbilledet er imidlertid under hurtig forandring, og PwC påpeger derfor at den nuværende indsats ikke er tilstrækkelig, idet der fremover vil være en øget risiko for brud på informationssikkerheden og It-sikkerheden i Københavns Kommune.

PwC har vurderet kommunens "modenhed" på området i forhold til sammenlignelige offentlige organisationer i det vestlige Europa og konklusionen er, at Københavns Kommune på en række centrale områder er mindre "moden" på It-sikkerhedsområdet end disse sammenlignelige organisationer.

PwC anfører 5 hovedområder som særligt opmærksomhedskrævende:

- Utilstrækkelig brugeradministration
- Manglende hændelsesoverblik
- Manglende fælles proces for risikostyring
- Manglende proces for forbedring af It-sikkerhed
- Utilstrækkelig implementering af sikkerhedstiltag i de enkelte forvaltninger.

Derfor har PwC givet en række konkrete anbefalinger til hvordan Københavns Kommune bør forbedre It-sikkerheden på kort og længere sigt.

Koncernservice har gennemgået anbefalingerne, der kan opdeles i:

1) Initiativer, der kan iværksættes med det samme

Digitalisering

Borups Allé 177
2400 København NV

EAN nummer
5798009809025

2) Initiativer, der håndteres i eksisterende projekter og indsatser
3) Initiativer, der kræver større investeringer og en mere langsigtet plan for implementering.

Handlingsplan til forbedring af It-sikkerheden
Koncernservice har allerede, efter at have modtaget rapporten fra PwC, igangsat arbejdet med at gennemføre alle initiativer der er identificeret under 1) og 2). Det sker i samarbejde med forvaltningerne.

Hovedparten af initiativerne forventes gennemført inden udgangen af 1. kvartal 2015. Der vil dog fortsat være arbejder i hele 2015 i forbindelse med konsolidering af de gennemførte løsninger.

Koncernservice arbejder derudover med at opstille en plan for nødvendige initiativer og investeringer på længere sigt. Denne plan vil danne baggrund for en indstilling til Økonomiudvalget, der forventes forelagt i 1. kvartal 2015.

Der er 5 hovedområder i den aktuelle handlingsplan.

1. **Adgangsstyring - systemadgang, tildeling, kontrol og afvikling (Brugeradministration/rettigheder/autorisationer).**
   Der arbejdes på at give bedre mulighed for ledelsestilsyn med rettigheder og forenkle de centrale arbejdsgange mest muligt. Indsatsen løber over hele 2015.

2. **Styring af informationssikkerhedsbrud (Hændelsesoverblik, logning/overvågning af trafik på netværk og centrale systemer, hændelser).**
   Der arbejdes på at forbedre overvågning af trafik på netværk og centrale systemer. Indsatsen løber over hele 2015.

3. **Risikovurdering- og håndtering (Systematisk risikostyring).**
   Der arbejdes på at etablere en proces til risikostyring, der muliggør prioritering mellem forskellige risici. Koncernservice vil indledningsvis anvende processen til at gennemgå de mest centrale systemer og processer i Københavns Kommunes samlede it-installation. Dette arbejde forventes gennemført inden udgangen af 1. kvartal 2015. Det konsoliderede koncept vil herefter blive tilbudt forvaltningerne til egen anvendelse.

4. **Fysisk sikring (Adgang til fysiske lokaliteter).**
   Der foreslås nedsat en ad hoc arbejdsgruppe med deltagelse af forvaltninger, Københavns Ejendomme og Koncernservice. Koncernservice udsender snarest invitation til at deltage i arbejdsgruppen, der forventes at påbegynde arbejdet i januar 2015. Arbejdsgruppen skal udarbejde paradigmer for fysisk sikring, dvs. etablere en fælles ramme for forvaltningernes vurdering af behov

for sikring af adgangsforholdene til kommunens bygninger. Den fælles ramme skal både kunne håndtere hensynet til at borgerne skal møde åbne og imødekommende kommunale tilbud og samtidig sikre at adgang til centrale netværk og installationer kan kontrolleres.

5. **Ansvarsplacering og organisering af indsatsen mellem Koncernservice og forvaltningerne.**
   PwC påpeger at der er behov for at tydeliggøre snitflader og ansvarsområder mellem Koncernservice og forvaltningerne. På Digitaliseringschefmødet 19. november 2014 blev det aftalt at nedsætte en ad-hoc arbejdsgruppe med deltagelse af forvaltningerne og Koncernservice med henblik på at vurdere arbejdsdeling og evt. behov for ændringer. Koncernservice vil i december 2014 fremlægge forslag til tidsplan og kommissorium for gruppen.

Koncernservice vil i samarbejde med forvaltningerne løbende sikre, at der i forhold til alle initiativer sker den fornødne afvejning mellem hensynet til It-sikkerhed og hensynet til tilgængelighed og funktionalitet.

Yderligere initiativer
Koncernservice vil med virkning fra januar 2015 etablere regelmæssig ledelsesinformation om aktuelle It-sikkerhedsmæssige problemstillinger.

Fremtidige redegørelser til Økonomiudvalg mv. vil beskrive det samlede trusselsbillede og fokusere mindre på konkrete enkelthændelser.

Aktuelle hændelser og trusler mod It-sikkerheden
Koncernservice har i dag ikke fuldt overblik over de faktiske hændelser på It-sikkerhedsområdet i Københavns Kommune. Koncernservice (It-sikkerhedsfunktionen) medvirker i udredning af konkrete hændelser efter anmodning fra forvaltningerne og fra 2015 vil information om de aktuelle hændelser indgå i den regelmæssige ledelsesinformation.

Koncernservice har aktuelt kendskab til at der i 2014 har været 7 tjenstlige personalesager vedr. It-sikkerhedshændelser, og der er i alt registreret 66 It-sikkerhedshændelser af meget varierende karakter i 2014.

De registrerede hændelser udgør imidlertid kun "toppen af isbjerget".

Kommunens netværk angribes konstant af eksterne hackere og kriminelle, der ønsker at anvende den kommunale infrastruktur til uvedkommende formål. Overvågning af netværkstrafikken viser

således forsøg på at etablere skjulte "trojanske heste", der kan anvendes til uvedkommende, typisk kriminelle formål rettet mod andre eksterne organisationer og som potentielt truer drifts- og datasikkerheden i Københavns kommune.

Kommunens netværk har 2 gange i 2014 været udsat for målrettede og koordinerede angreb, og kommunens firewall afviser dagligt mere end 100.000 uvedkommende mails.

Der er alene i den seneste måned afvist i alt 6510 forskellige virus.