



21-08-2015

Til Økonomiudvalget (aflæggerbordet)

Sagsnr.
2014-0205519

Orientering vedr. It-sikkerheden

Dokumentnr.
2014-0205519-30

Sagsbeskrivelse

Borgerrepræsentationen besluttede 30. april 2015 (Dagsordenens punkt 9) at Koncernservice skulle iværksætte Handlingsplan til styrkelse af It-sikkerheden.

Sagsbehandler
Jens Ingemann

Aktiviteterne vil forbedre it-sikkerheden i alle dele af Københavns Kommune og lette arbejdsbyrden væsentligt for både systemejere og for decentrale ledere i alle forvaltninger.

Handlingsplanen blev udarbejdet efter ekstern vurdering af it-sikkerhedsniveauet i Københavns Kommune, dvs. både i KS og i forvaltningerne, som blev udført af konsulentfirmaet PwC i sommeren 2014. Undersøgelsen viste, at Københavns Kommune havde en række helt konkrete udfordringer, som det var nødvendigt at løse hurtigst muligt.

Koncernservice fremlægger hermed (1) oversigt over allerede opnåede forbedringer på hovedområderne i handlingsplanen og (2) en tidsplan for implementering af udestående aktiviteter.

1. Allerede opnåede forbedringer

- Styring af informationssikkerheden: Det blev besluttet at anskaffe en løsning, der muliggør central overvågning af aktiviteter på den centrale It-infrastruktur og i de væsentlige fagsystemer.

Den nye løsning fra firmaet Logpoint er sat i drift og har allerede givet grundlag til at reagere overfor hændelser på netværket. Sikkerheden er øget ved at systemet logger aktivitet og giver alarm, hvis hændelser afviger fra normalbilledet og dermed vil identificering af og reaktion på fx hackerangreb eller andre trusler mod driftssikkerheden hurtigere kunne finde sted. I løbet af september etableres samlet logningsoverblik over trafik og hændelser på hele den centrale It-infrastruktur og i løbet af 4. kvartal på centrale fagsystemer som driftafvikles af KS. I 4. kvartal udvikles rapporter, som kan give systemejere og andre det nødvendige overblik, og grundlaget er dermed skabt for at rulle løsningen ud over forvaltningernes fagsystemer fra 2016. Som led i

Enhedschef

Borups Allé 177
2400 København NV

Telefon
26114651

EAN nummer
5798009809308

www.kk.dk

Handlingsplanen har KS fra 2016 fået mulighed for at ansætte ekstra medarbejdere til at håndtere denne nye opgave.

- Styring af lokale administrationsrettigheder: Det blev besluttet at der skulle etableres et samlet overblik over brugere med administrative rettigheder og at det skulle sikres, at de pågældende kun har administrative rettigheder til systemer, som er nødvendige for at de kan udføre deres arbejdsopgaver. Der er anskaffet et nyt It-værktøj til formålet, og det er med udgangen af august 2015 indført for brugere i 6 ud af 7 forvaltninger. Den sidste forvaltning overgår efter eget ønske først til den nye løsning i løbet af september. Dermed er sikkerheden forøget væsentligt, idet de pågældende dermed ikke tilsigtet eller utilsigtet kan ændre i opsætning af ikke arbejdsrelevante systemer på egen PC.
- Ekstern overvågning af hændelser på netværket: Det blev besluttet at indføre central overvågning af hvilke hjemmesider og IP-adresser, der sender henvendelser til Københavns Kommunes netværk og omvendt. Løsningen er sat i drift og muliggør blokeringer af utroværdige hjemmesider. Herved etableres et løbende overblik over aktuelle trusler og uautoriserede hændelser, og log fra systemet vil fra september indgå i Logpoint løsningen (beskrevet ovenfor). Derved muliggøres proaktive reaktioner med henblik på eliminering af trusler, inden disse bliver til konkrete hændelser. It-sikkerheden er således øget internt i kommunen og også eksternt, idet det forhindres at kommunens udstyr kan bruges til uvedkommende formål som f.eks. som base for cyberangreb på 3. parts installationer.
- Webscanner: Det blev besluttet at der skulle indføres en forbedret mulighed for centralt at overvåge, om personhenførbare oplysninger utilsigtet offentliggøres på kommunens borgerrettede hjemmesider. Løsningen er sat i drift og har allerede vist sin værdi ved i flere tilfælde at finde dokumenter indeholdende personhenførbare oplysninger, som fejlagtigt var offentliggjort på kk.dk. Disse dokumenter er herefter straks fjernet.

2. Tidsplan for implementering af udestående aktiviteter

Koncernservice har jf. ovenfor sikret at de besluttede aktiviteter er igangsat umiddelbart efter frigivelse af bevillingen i Borgerrepræsentationen.

Implementering afsluttes i 2015, og opfølgende aktiviteter håndteres i drift af løsningerne i 2016 og frem.

Koncernservice fremlægger ved årsskiftet 2015/2016 ny indstilling til Økonomiudvalget vedr. mulighederne for automatisering af adgangsstyring og forbedring af lederes tilsyn med medarbejderes rettigheder til systemadgange. Det vil ske ud fra den igangværende analyse med opstilling af Business case på området.

Aktuel status for implementering af aktiviteterne er beskrevet i nedenstående tabel:

| Aktivitet | Beskrivelse | Status pr. 1. september 2015 | Deadline |
|--|---|---|----------------------|
| Styring af informationssikkerhed gennem anskaffelse og drift af en log- og event management-løsning (SIEM) | Systemet implementeres og centrale fælles systemer i KS overvåges | Forventes afsluttes til aftalt deadline | Ultimo december 2015 |
| | Udbygning af løsning med fag-applikationer fra forvaltningerne sker i en kontinuerlig proces som led i driften af løsningen fra 2016, således at systemer løbende inddrages i overvågningen | | |
| Etablering af ny struktur på datanetværket | Ændring skal være gennemført | Forventes afsluttes til aftalt deadline | Ultimo december 2015 |
| Styring af lokale administrations-rettigheder | Overdragelse til fuld drift | I drift for 6 ud af 7 forvaltninger ultimo august, den sidste forvaltning følger efter eget ønske i september. | Ultimo august 2015 |
| | | | |

| | | | |
|---|---|--|----------------------|
| Ekstern overvågning af hændelser på netværket | Overdragelse til fuld drift | Er i drift | Ultimo august 2015 |
| Webscanner | Overdragelse til fuld drift for kk.dk | Er i drift | Primo september 2015 |
| | Fortsat udbygning af løsning med nye KK drevne sites - kontinuerlig proces som led i drift af løsning | | |
| Foranalyse og etablering af business case vedr. automatisering af adgangsstyring. | Foranalyse med opstilling af business case skal være gennemført | Forventes afsluttes til aftalt deadline | Ultimo november 2015 |
| | Indstilling til ØU | Forventes leveret til aftalt deadline | Primo januar 2016 |

Koncernservice afrapporterer fremdrift i projektet ca. hver 3. måned, næste gang i forbindelse med fremlæggelse af ny indstilling til Økonomiudvalget.