KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncernservice

NOTAT

16-03-2015

Sagsnr.
2014-0205519

Dokumentnr.
2014-0205519-8

Sagsbehandler
Mette Høgholt Lønne

Til Økonomiudvalget

Bilag 1 til indstilling til Økonomiudvalget

Uddybning vedr. Købehavns Kommunens modenhed på It-sikkerhedsområdet

Konklusionen i PWCs rapport lød, at Københavns Kommune hidtil har anvendt fornuftige rutiner til styring af It-sikkerheden ud fra et traditionelt trusselsbillede, men at trusselsbilledet er under hurtig forandring.

Koncernservice har i 2014 på baggrund af undersøgelsen udarbejdet en handlingsplan for at gennemføre alle initiativer, der kunne iværksættes med det samme eller kan indarbejdes i eksisterende projekter og initiativer.

Det vil imidlertid - som fremlagt i indstillingen - være nødvendigt at afsætte nye anlægs- og driftsmidler for at kunne gennemføre alle elementer i planen.

Københavns Kommune har været It-sikkerhedsmæssigt på forkant med veldokumenterede processer og en udbygget It-sikkerhedspolitik, men det er ikke længere tilstrækkeligt. Koncernservice vurderer, at de foreslåede løsninger udgør en kommende de-facto standard for store offentlige og private organisationer og at Københavns Kommune er nødsaget til at gennemføre de foreslåede investeringer. Region Hovedstaden og Codan er eksempler på organisationer, der allerede har foretaget de nødvendige investeringer, mens f.eks. Skat er i forberedelsesfasen.

Et konkret eksempel på det ændrede risikobillede er det hackerangreb, Københavns Kommune blev udsat for i januar 2015, hvor en medarbejder i SUF åbnede en inficeret mail med "ondsindet" indhold og flere tusinde filer blev beskadiget. Fra angrebet startede til det blev opdaget gik der halvanden dag. Hvis Københavns Kommune havde haft systemerne til at monitorere sådanne hændelser, kunne angrebet have været stoppet langt tidligere. Det lykkedes dog at afværge yderligere skade ved en hurtig indsats og Koncernservice har reetableret filerne fra back-up. Københavns Kommune var blot en af flere offentlige myndigheder, der blev angrebet.

Risikoen er øget i alle dele af Københavns Kommune, idet driftsansvaret er placeret hos forvaltningerne (og herunder KS som driftsansvarlig for den centrale infrastruktur). Direktionerne i alle forvaltninger skal jf. det gældende It-sikkerhedsregulativ til enhver tid

Ledelsessekretariatet

Borups Allé 177
2400 København NV

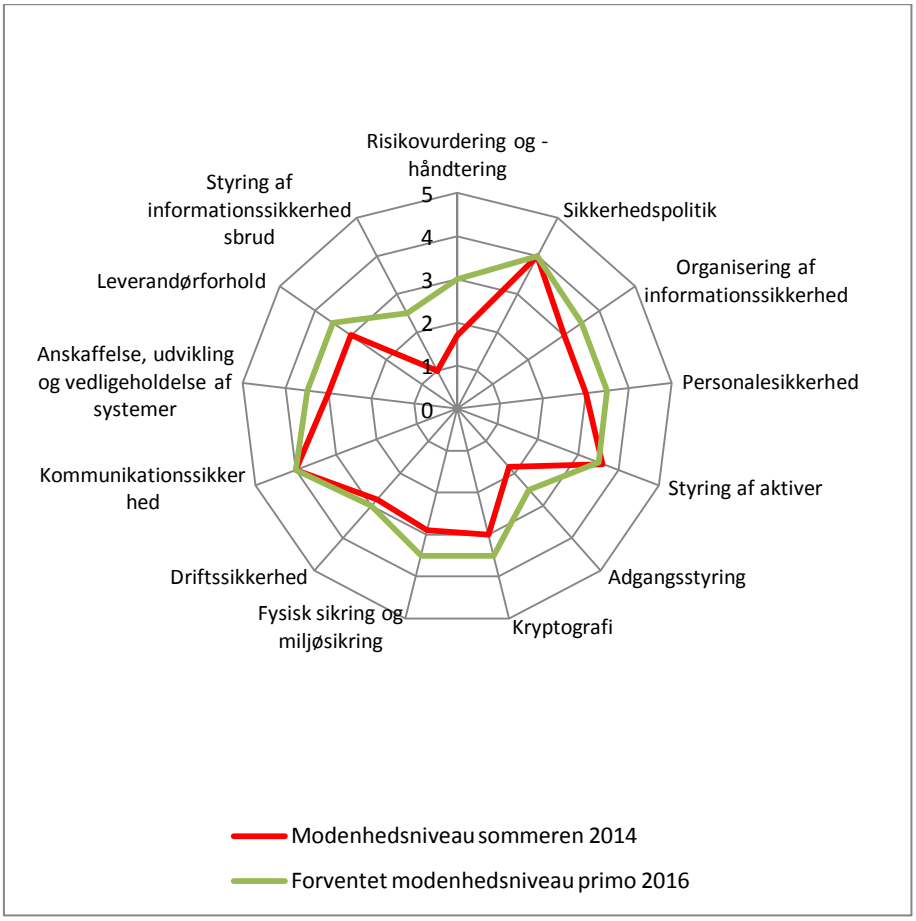
Telefon
2169 3046

EAN nummer
5798009809117

sikre, at de daglige arbejdsgange lever op til lovgivningskrav til håndtering af person- og værdidata.

Det nye trusselsbillede betyder at der er en væsentlig forøget risiko for at den enkelte forvaltning står overfor hidtil usete brud på informationssikkerheden.

Faktisk modenhedsniveau sommeren 2014 og forventet modenhed primo 2016 (efter gennemførelse af de foreslåede aktiviteter i 2015-2016).



Figuren viser, at modenheden aktuelt er forskellig på de enkelte sikkerhedsområder. De foreslåede aktiviteter i 2015-16 fokuserer på at hæve sikkerhedsniveauet der, hvor Københavns Kommunes modenhed er lavest, dvs. risikovurdering og -håndtering, styring af informationssikkerhed samt adgangsstyring og dermed påbegynde den nødvendige forbedring af niveauet på de prioriterede områder. Dernæst vil der fortsat være behov for yderligere initiativer i 2017 og frem for at nå op på den ønskede modenhed på 4.

Aktiviteter over en flerårig periode

Allerede igangsatte aktiviteter:

- Risikostyring med fælles model for risikovurdering. Koncernservice har i 2014 afholdt omkostningerne til at etablere en konsolideret risikostyringsproces. Forvaltningerne tilbydes i 2. kvartal 2015 at indgå i risikostyringsprocessen, og få vurderet It-sikkerheden i egne fagsystemer. Risikovurderingen udmøntes i en ledelsesrapport der beskriver It-sikkerhedsmæssige risici og præsenterer evt. mulige foranstaltninger for at forbedre It-sikkerheden. I løbet af 2015 etableres et årshjul, så de konkrete risici kan vurderes med regelmæssige mellemrum.
- Vurdering af samarbejdet mellem forvaltningerne og Koncernservice om It-sikkerhed, herunder vurdering af behov for tilpasning af It-sikkerhedsregulativ og arbejdsdeling.

Nye nødvendige aktiviteter til iværksættelse snarest muligt

a. Styring af informationssikkerhed gennem anskaffelse og drift af en log- og event management-løsning (SIEM – Security Information and Event Management) som grundlæggende forudsætning for, at Koncernservice kan overvåge og beskytte de centrale dele af IT-infrastrukturen, hjælpe systemejere på centrale systemer samt store fagsystemer i alle forvaltninger med at overvåge anvendelse og så vidt muligt håndtere konkrete trusler mod driftssikkerheden allerede i et cyberangrebs indledende faser.

   En SIEM-løsning indeholder bl.a. følgende funktioner:

   - Support af driften med avanceret fejlfinding
   - Monitorering af sikkerhedshændelser
   - Værktøjer der muliggør effektiv efterforskning og bevissikring i tilfælde af kriminalitet
   - Alarmering ved misbrug af systemer og rettigheder
   - Monitorering af anvendelse af tilgang til personfølsomme data
   - Forbedring af ledelsesinformation på baggrund af større datamængder på tværs af systemer.

   En SIEM-løsning skaber grundlaget for at overvåge hændelser på netværket og sikre at det kun er medarbejdere fra Københavns Kommune, der bruger netværket. Med en SIEM-løsning bliver det ligeledes muligt at efterforske utilsigtede hændelser såsom bedrageri- og hackersager og dermed afværge trusler mod driftssikkerheden.

   Det vil være nødvendigt at afsætte 2½ nye årsværk til at udnytte mulighederne i et SIEM-system fuldt ud, således at systemejere og forvaltningerne kan serviceres som beskrevet.

b. Etablering af ny struktur på datanetværket.
Risikoen for uautoriseret benyttelse af administrative netværksstik reduceres markant ved at etablere en ny struktur på datanetværket.

c. Lokale administratorrettigheder. Anskaffelse af et system, der kan styre lokale administrationsrettigheder uden at serviceniveauet for den enkelte bruger reduceres.

d. Ekstern overvågning af hændelser på netværket (Secure DNS)
Der etableres et løbende overblik over aktuelle trusler og uautoriserede hændelser. Derved er det muligt at reagere proaktivt og umiddelbart med henblik på at eliminere trusler inden de bliver til konkrete hændelser. IT-sikkerheden øges dermed internt i kommunen og også eksternt, idet det så kan forhindres, at kommunens udstyr bruges til uvedkommende formål som f.eks. som base for cyberangreb på 3. parts installationer.

e. Webscanner
Der etableres mulighed for at foretage løbende overvågning og scanning af hjemmesider for CPR-numre mv., som fejlagtigt offentliggøres på eksterne og interne hjemmesider. IT-sikkerheden forbedres idet evt. fejl løbende vil blive opdaget og dermed kan udbedres umiddelbart.

f. Foranalyse og etablering af business case vedr. automatisering af adgangsstyring. Der skal etableres beslutningsgrundlag vedr. mulig anskaffelse af et Identity Access Management (IAM) system, der ved automatiserede processer kan erstatte de nuværende manuelle rutiner til håndtering af adgangsstyring i Koncernservices brugeradministration. Det skal afklares om en IAM-løsning er det rigtige valg til at håndtere de identificerede problemer med adgangsstyring til systemer og ledelsestilsyn med autorisationer.
Der vil samtidig blive indhentet yderligere referencer fra andre store organisationer, der har implementeret lignende løsninger.
Det forventes at der kan opnås en væsentlig effektivisering ved at automatisere eksisterende manuelle arbejdsgange, og en automatiseret løsning vil gøre det muligt at forenkle ledelsestilsynsopgaven for alle personaleansvarlige ledere, der i dag med manuelle rutiner skal føre tilsyn med, at medarbejdere kun har de rettigheder til systemer, som deres aktuelle arbejdsfunktion giver anledning til. Det vil være muligt at definere tildeling af autorisationer ud fra definerede roller og medarbejdertyper, og tilsynet vil dermed kunne automatiseres i meget høj grad.

Der kan overvejes flere mulige scenarier for en hensigtsmæssig implementering, som tager højde for kompleksiteten i Københavns Kommunes systemlandskab.

Derfor foreslås arbejdet påbegyndt med en foranalyse i 2015, således at der ultimo 2015 foreligger beslutningsgrundlag i form af en business case og model for implementering og drift af en hensigtsmæssig løsning. På baggrund af foranalysen vil Koncernservice udarbejde en ny indstilling til Økonomiudvalget til behandling primo 2016.

g. Indstillingen til Økonomiudvalget primo 2016 vil også omfatte evt. yderligere initiativer på baggrund af udvikling i trusselsbillede og på baggrund af evt. ændret lovgivning i forlængelse af kommende EU-forordning om persondata mv.

Overførelse af ansvaret for overvågnings- og opfølgningsopgaven vedr. logning fra forvaltningerne til Koncernservice
Som led i anskaffelse af en såkaldt SIEM-løsning, jf. punkt a. ovenfor, foreslås det fra 2016 løbende at overføre ansvaret for overvågnings- og opfølgningsopgaven vedr. logning fra forvaltningerne til Koncernservice.

Systemejerne i alle forvaltninger er jf. sikkerhedsregulativet ansvarlige for at opsætte alle systemer med person- og værdidata, så anvendelsen logges og det er muligt at overvåge og i nødvendigt omfang følge op på de aktiviteter, der foregår i forhold til det enkelte system. Koncernservice kontrollerer i forbindelse med It-anskaffelsesprocessen at der etableres logningsmulighed for alle relevante systemer, men det er efterfølgende meget vanskeligt for systemejeren manuelt at overvåge trafikken på de enkelte systemer.

En stikprøve fra 2014 viser, at systemejere typisk først følger op, når der er en konkret anledning. Med det nye trusselsbillede vurderer Koncernservice, at det er nødvendigt i videst muligt omfang at automatisere og centralisere den løbende overvågning og dermed overføre ansvaret for overvågnings- og opfølgningsopgaven fra forvaltningerne til Koncernservice.

Det vil jf. It-sikkerhedsregulativet stadig være forvaltningernes ansvar at sikre, at systemer med person- og værdidata er opsat, så det er muligt at foretage logning af trafikken.
SIEM løsningen giver mulighed for en central og samlet overvågning i Koncernservice. Den samlede overvågning skal sikre at forvaltningernes ledelse alarmeres når brugere foretager mistænkelige opslag på person- eller værdidata, samt ved mistanke om misbrug af kommunens systemer.