REFERAT Direktionen d. 03-04-2018

Mødedato	Tirsdag d. 03. april 2018 kl. 12:30
Mødested	Mødelokale B105
Mødedeltagere	Lars Holte, Jørgen Lerhard, Per Aalbæk Nielsen, Charlotte Markussen, Kathrine Seier Skaastrup (sekretær)

Indholdsfortegnelse

Punkt 1: Øvrige sager 03-04-2018

17/22360

Punkt 2: Økonomiopfølgning 3-04-2018

17/22360

Punkt 3: Lukket

17/22668

Punkt 4: Overordnet informationssikkerhedspolitik

17/15311

Baggrund

Høje-Taastrup Kommunes it-sikkerhedspolitik har ikke hidtil været baseret på ISO 27001, og derfor fremlægges denne sag med en ny overordnet informationssikkerhedspolitik og informationssikkerhedshåndbog baseret på denne standard, da KL's oplæg til sikkerhedsprogram forudsætter at kommunerne har en sikkerhedspolitik og en sikkerhedshåndbog, som er baseret på ISO 27001.

Den nye sikkerhedspolitik- og håndbog afløser de hidtidige dokumenter "retningslinjer og regler for it-sikkerhed" og "it-sikkerhedshåndbogen", som senest er godkendt i Økonomiudvalget 8-11-2016.

Sikkerhedspolitikken og sikkerhedshåndbogen skal fortsat forelægges årligt til godkendelse i Økonomiudvalget. Fremadrettet vil det i højere grad være muligt kun at referere til evt. ændringer.

Indstilling

ØDC indstiller at direktionen godkender og indstiller

-den vedlagte informationssikkerhedspolitik (bilag 1),

-den vedlagte informationssikkerhedshåndbog (bilag 2),

til økonomiudvalgets godkendelse (bilag 3)

og at direktionen godkender

-at der nedsættes et informationssikkerhedsforum jf. vedhæftede bilag 4 og 5

Beslutning Direktionen den 03-04-2018

Direktionen tilsluttede sig sagen med enkelte rettelser.

Sagsfremstilling

I takt med den øgede digitalisering i samfundet i øvrigt vokser truslen mod hele den offentlige sektors it-systemer og data, hvilket stiller større krav til datasikkerheden. Vi er truet af udefrakommende hackerangreb, ligesom medarbejderne selv kan udgøre en risiko, hvis de bevidst eller ubevidst misbruger deres adgang til it-systemer og data.

Derfor bør HTK dels have etableret grundliggende sikringstiltag, der beskytter mod bl.a. hackerangreb, dels styre og kontrollere medarbejdernes adgang til it-systemer og data. Det gælder særligt i forhold til de medarbejdere, der har privilegerede rettigheder og dermed fuld adgang til og kontrol med it-systemerne, idet et hackerangreb mod disse medarbejdere vil give hackeren samme adgang og kontrol. De grundliggende sikringstiltag kan sammen med styring og kontrol af privilegerede rettigheder i væsentlig grad reducere risikoen for, at vores it-systemer og data kompromitteres. Ofte er det en kombination af f.eks. svagheder i it-systemer og forkert medarbejderadfærd, der medfører brud på it-sikkerheden og dermed risiko for, at data kompromitteres.

KL har beskrevet nødvendigheden af, at der arbejdes for at styrke kommunernes datasikkerhed. I KL's oplæg til sikkerheds program forudsættes det at kommunerne har en sikkerhedspolitik og en sikkerhedshåndbog som er baseret på ISO 27001[1], som er en international standard for datasikkerhed. Høje-Taastrup Kommunes sikkerhedspolitik har ikke hidtil været baseret på denne standard. Det iværksatte sikkerhedsprogram fra KL, følger Høje-Taastrup Kommune gennem DSD (Den storkøbenhavnske Digitaliseringsforening). I den opgave arbejder vi sammen med DSD for at få synergieffekt i de tiltag, som hver kommune kommer op med, og så erfaringer og ideer kan deles mellem medlemskommunerne. Dette er af stor værdi, da opgaven med sikkerhed som oftest ligger på enkeltpersoner uden megen mulighed for faglig sparring indenfor kommunens rammer.

I forbindelse med vedtagelsen af den nye persondatabeskyttelsesforordning (GDPR) er der en række nye forhold HTK skal tage i betragtning, og der er en række forhold i den gældende lovgivning, som skal genbesøges og revitaliseres i organisationen. Af de nye forhold er der en væsentlig skærpelse i forhold til, hvordan kommunen skal forholde sig til

hændelser (sikkerhedsbrud). Kommunen skal reagere både hurtigt og ærligt. Dette skal ses i sammenhæng med den styrkede retsstilling, som borgeren har i den nye lovgivning. Samtidig er der en række gældende lovgivninger, som kommunen skal gennemgå, for at se om denne overholdes på den måde, som loven hidtil har foreskrevet, og om de procedurer for overholdelse er i overensstemmelse med best practice. Disse processer og procedurer vil fremadrettet blive gennemløbet med alle centre med særligt fokus på de centre, som behandler følsomme personoplysninger.

Samtidig skal vi sikre, at alle data opbevares korrekt, så de ikke bliver tilgængelige for andre end de personer, som skal anvende data i deres sagsbehandling, og som skal have adgang til dem for at kunne lave en korrekt afgørelse til vores borgere og virksomheder.

Sikkerhedsprocesserne og det øgede fokus på borgernes rettigheder gør også, at vi skal sørge for, at vores ansatte alle bliver bekendte med reglerne og i de tilfælde, hvor data er følsomme, også giver vores ansatte de bedste redskaber til at overholde lovgivningen.

Den nye informationssikkerhedspolitik og håndbog er sat lidt anderledes op end de hidtidige dokumenter. Det skyldes, dels overgangen til ISO 27001, og dels fordi udarbejdelsen nu er systemunderstøttet. Flere af de øvrige kommuner i DSD har samme system og baserer sig på samme skabelon, hvilket er en fordel i forhold til vores kommende samarbejde med den fælles databeskyttelsesrådgiver. Da informationssikkerhedshåndbogen er ganske lang og ikke specielt let tilgængelig, vil ØDC i løbet af 1. halvår 2018:

1) gennemarbejde vores eksisterende korte sikkerhedspjece, som er målrettet medarbejdere. Pjecen lægges på MitHTK og vil være obligatorisk læsning for alle medarbejdere.

2) Kommunikere til ledere i forhold til, hvilke afsnit af sikkerhedshåndbogen ledere skal kende. (evt. i form af et særskilt dokument, som er mere læsevenligt)

Datasikkerhedsforum

Da der er behov for at arbejde med sikkerhed på tværs af hele kommunen, har KL anbefalet, at kommunerne nedsætter et særligt organ, som arbejder med sikkerhed. Et sådant organ bør efter ØDCs opfattelse nedsættes med deltagelse af de centre, som har en særlig interesse i sikkerhed og er særligt belastet med data af følsom karakter. Disse centre er BAC, SHC, SOUC, BURC og ISC. Der henvises til vedlagte bilag 4 og 5.

Med en sikkerhedspolitik baseret på ISO 27001 opruster kommunen på målsætningerne på sikkerhedsfronten over en bred kam. Det indebærer, at der forestår et implementeringsarbejde for at leve op til standarden. Der skal laves sikkerhed, som sikrer mod, at uvedkommende kommer ind i vores systemer, og der skal laves tiltag, som uddanner og bevidsthedsgør vores medarbejdere, så de vil få lettere ved at gennemskue forsøg på at få adgang til vores systemer. Processen med konkret at løfte organisationen vil blive forelagt informationssikkerhedsforummet. Der er primært tale om skærpelser, som vi nu – i forlængelse af GDPR – sætter fokus på, og som vi i et eller andet omfang burde have haft fokus på tidligere. Fx jævnlig gennemgang af logfiler og rapportering på sikkerhedshændelser.

Den øgede indsats betyder herudover, at direktionen fremover vil blive inddraget hyppigere end tidligere (hvor det kun er sket i forbindelse med årlig forelæggelse af it-sikkerhedspolitikken). Dels er der brug for at direktionen informeres om fremdrift og dels kan der være indstillinger fra datasikkerhedsforummet som bør forelægges direktionen.

---

[1] At informationssikkerhedspolitikken er baseret på ISO 27001 standarden er ikke det samme som at kommunen er certificeret efter ISO standarden. En certificering vil kræve en meget større ressourceindsats og det vurderes ikke at stå mål med udbyttet.

Bilag

overordnet sikkerhedspolitik 2018.pdf

Sikkerhedshåndbog 2018 m. indholdfortegnelse.pdf

Udkast ØU sag Godkendelse af overordnet informationssikkerhedspolitik

Datasikkerhedsforum - baggrund

Datasikkerhedsforum - kommisorium

Punkt 5: Årshjul 3-4-2018

17/22360

Baggrund

Vedlagt årshjul for direktionens mødesager for 2018. Hermed løbende aktiviteter for 2018:

Borgmesterens deltagelse (kvartalsvis) i direktionsmøder
(16. april)
(14. maj)
11. juni
20. august
(17. september)
8. oktober
(12. november)
3. december

Direktionens heldagsmøder 2018
16. april
14. maj
18. juni
13. august
17. september
22. oktober
12. november
10. december

Chefforum-seminarer 2018
9. 10. april

30.-31. august

Bilag:

1	Åben	Årshjul 2018 - Direktionen	124744/17

Bilag

Årshjul 2018 - Direktionen