Region Hovedstaden

Center for It, Medico og Telefoni

NOTAT

Til: Regionsrådet

Journal-nr.: 16043917

Dato: 24. januar 2018

Uddybende forklaring til udkast til udtalelse fra Regionsrådet

På Forretningsudvalgets møde den 23. januar 2018 blev der stillet spørgsmål til en række af de beskrevne tiltag og tidspunkterne for deres færdiggørelse.

Administrationen kan oplyse følgende uddybende om indholdet:

Privilegerede rettigheder
Det højeste niveau af rettigheder, adgang og kontrol over organisationens it-systemer og data. Desuden kan de privilegerede rettigheder i særlige tilfælde give mulighed for at omgå institutionens sikringsforanstaltninger. I nogle tilfælde kan de privilegerede rettigheder – afhængigt af organisationens systemopbygning – også give adgang til andre væsentlige it-systemer og data. Privilegerede rettigheder betegner i denne sammenhæng de it-medarbejdere og/eller system- og servicekonti, der er medlem af "Domain Admins-gruppen".

System- og servicekonti
Anvendes bl.a. til automatiserede kørsler i it-driften. Det kan fx være periodiske overførsler af data, backupkørsler og overvågning af it-driften. System- og servicekonti har tilknyttet nogle rettigheder, som bestemmer, hvad kontoen kan bruges til. Rettighederne for de enkelte system- og servicekonti er normalt stærkt begrænsede til alene at udføre den specifikke opgave.
De system- og servicekonti, der beskrives i denne sammenhæng, har privilegerede rettigheder.
System- og servicekonti er brugeruafhængige. Hver system- og servicekonto har ét password, som betroede it-medarbejdere typisk har kendskab til. System- og servicekonti anvendes dermed ikke med et personligt password. Al anvendelse af system- og servicekonti, herunder misbrug, er derfor ikke personhenførbar.

Logning
Alle handlinger på regionens it-systemer genererer et digitalt fingeraftryk, som kan opsamles i en log. Logning af konti med privilegerede rettigheder kan fx ofte vise, om

personer har logget sig på it-systemer, og hvad de har brugt rettighederne til. Logning øger chancen for at kunne undersøge uregelmæssigheder/sikkerhedsbrud til bunds.

Idet der er tale om tre forskellige tiltag, er der derfor også tale om tre forskellige tidspunkter for forventet færdigimplementering/delimplementering.

Tiltagene relaterer sig til disse tre kritikpunkter:

1. At Region Hovedstaden ikke har sikret, at medarbejdere med privilegerede rettigheder ikke kan gå på nettet, når de er logget på med deres privilegerede rettigheder
2. At Region Hovedstaden ikke har sikret, at alle system- og servicekonti har autogenererede passwords og at dette er systemunderstøttet
3. At Region Hovedstaden ikke logger, når brugere med privilegerede rettigheder starter programmer, men kun, at de logger af og på.

Der er dermed tale om tre forskellige tiltag:

Ad 1)
Sikring af, at medarbejdere med privilegerede rettigheder ikke kan gå på nettet, når de er logget på med deres privilegerede rettigheder – forventes færdigimplementeret i første kvartal 2018.

Ad 2)
Sikring af, at system- og servicekonti har autogenererede passwords og at dette er systemunderstøttet – forventes færdigt i første kvartal 2018.

Ad 3)
Etablering af logning, når brugere med privilegerede rettigheder starter programmer – første fase af implementeringen forventes færdig med udgangen af 2018.

Administrationen har desuden lavet en redaktionel ændring i udkastet til udtalelsen, så det nu fremgår hvilke afsnit på side 2, der henviser til de tre bullets med de væsentligste kritikpunkter.