Koncern IT
Økonomiforvaltningen

Notat

Til ØU

Kontrol med ureglementerede opslag i CPR og øvrige it-systemer med følsomme personoplysninger

15. marts 2021

Sagsnummer
2021-0032146

Dokumentnummer
2021-0032146-5

Baggrund
For at forhindre misbrug af kommunens it-systemer, herunder systemer, der rummer CPR-oplysninger, overvåges og kontrolleres it-systemernes logdata i Københavns Kommune (KK).

Hjemmelsgrundlag
Det fremgår af databeskyttelsesforordningens artikel 32, stk. 1, at dataansvarlige (i dette tilfælde KK) skal gennemføre de nødvendige tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der kan være, når dataansvarlige behandler personoplysninger.

Ansvar og kontrol
Den systemansvarlige kontorchef for et system er ansvarlig for, at der gennemføres periodiske udtræk fra systemer for f.eks. at kontrollere hvilke brugere, der har adgange til data og systemet samt hvilke handlinger, brugerne har udført.

Automatiseret Logopfølgning
Mange store virksomheder og organisationer har så kompleks en it-infrastruktur, at det kan være svært og tage lang tid at opdage misbrug af de enkelte it-systemer og øvrige sikkerhedstrusler. Derfor har KK anskaffet et såkaldt SIEM-system (Security Information and Event Management-system), der samler logdata fra administrative systemer, netværksudstyr og sikkerhedsudstyr ét sted, hvorfra der kan foretages analyser gennem logfiler og sættes alarmer op ved uregelmæssig anvendelse.

Københavns Kommunes SIEM-system er i fuld drift og anvendes af alle forvaltninger til at forbedre monitoreringen af anvendelsen af udvalgte fagsystemer og centrale infrastruktursystemer.

Koncern IT har desuden i 2020 færdigudviklet et automatisk kontrolmodul i SIEM, som kan alarmere på CPR-opslag på nære relationer (fx ægtefælle, ekspartner, børn) i 12 særligt udvalgte fagsystemer. Der er desuden udarbejdet en fællesadministrativ forretningsgang, der skal understøtte anvendelsen af løsningen til alle forvaltninger. Løsningen tages i brug i 2. kvartal 2021.

Opfølgning på logning
Det konkrete arbejde med at følge op på den logning, der foretages i KK sker overordnet på tre måder:

1. Automatiseret i KK's SIEM løsning, hvor der med udgangspunkt i foruddefinerede 'use cases' sendes enten regelmæssige rapporter, eller specifikke alarmer til systemejeren i forvaltningen.

2. Semi-automatiseret i KK's SIEM løsning, hvor der med udgangspunkt i enten en konkret mistanke eller løbende stikprøvekontrol kan fremsøges data i gemte logs for at undersøge en given brugers adfærd

3. Manuelt i det enkelte fagsystems logfil, hvor den systemansvarlige chef har ansvaret for at sikre en løbende stikprøvekontrol med brugerhandlinger i det givne system.

Ad 1. Eksempel på automatiseret logopfølgning
Med henblik på at konkretisere ovenstående overordnede beskrivelse af, hvordan opfølgningen på logningen foregår i KK, følger herunder et konkret eksempel på automatiseret logopfølgning i CURA (elektronisk omsorgsjournalsystem i SUF).

Den primære logopfølgning i CURA drejer sig om den såkaldte 'værdispringsregel', som kort fortalt handler om, hvorvidt medarbejdere i SUF retmæssigt fremsøger, læser og/eller journaliserer oplysninger på borgere, som de har arbejdsmæssigt behov for. KIT har i den forbindelse i et tæt samarbejde med SUF udarbejdet fire 'use cases', som via systemets logfil via SIEM kan rapportere på følgende:

1. Kontrol af brugen af værdispring for de medarbejdere som har tilladelse til at foretage værdispring. Formålet er at monitorere, om der er medarbejdere, som foretager værdispring uhensigtsmæssigt ofte. Systemejer i SUF modtager en månedlig rapport fra SIEM i KIT
2. Kontrol af brugen af værdispring for de medarbejdere, der som udgangspunkt ikke må foretage værdispring, men som undtagelsesvist kan have et særligt situationsbestemt behov. Formålet er at monitorere antallet af aktiverede værdispring og følge op på uregelmæssigheder. Systemejer i SUF modtager en ugentlig rapport fra SIEM i KIT
3. Kontrol af brugen af værdispring for de medarbejdere, som ikke har tilladelse til at foretage værdispring. Disse medarbejdere kan i yderste nødstilfælde være tvunget til at foretage værdispring. Formålet er at monitorere hvert tilfælde og føre kontrol. Systemejer i SUF modtager en daglig rapport fra SIEM i KIT
4. Generel kontrol og statistik med alle værdispring i SUF. Systemejer i SUF modtager en månedlig rapport fra SIEM i KIT med oversigt over alle værdispring og deres fordeling på kategorier ovenfor.

Ad 2 og 3. Semiautomatisk eller manuel logopfølgning
Koncern IT's risikovurderinger af kommunens it-systemer i 2020 har vist, at der på nogle områder er udfordringer med den manuelle logkontrol, hvor der bl.a. er set eksempler på, at der mangler processer og dokumentation for, at der er gennemført de nødvendige kontroller.

I forbindelse med risikovurderingerne udarbejder alle forvaltninger handleplaner, der redegør for, hvordan og hvornår forvaltningerne retter

op på eventuelle udfordringer. Derfor er der allerede fastlagt deadlines for, hvornår samtlige udeståender skal være løst på området.

Resultatet af risikovurderingerne er sammen med handleplanerne præsenteret for IT-kredsen (et tværgående forum for forvaltningernes it-direktører), hvor der på tværs af alle forvaltninger er enighed om, at der skal ske en fokuseret indsats på området. Det er desuden aftalt med kommunens DPO (Data Protection Officer), at Koncern IT følger op på området igen allerede medio 2021.

Sammenfatning
Som det fremgår af ovenstående, har kommunen iværksat en række tiltag – både automatiske, semiautomatiske og manuelle kontroller, der skal sikre, at kommunen kontrollerer, om der sker ureglementerede opslag på CPR og andre systemer med følsomme personoplysninger.

KK har desuden fokus på området fremover og følger op på eventuelle udeståender i forhold til manuelle processer og dokumentation af gennemførte kontroller.