Koncern IT
Økonomiforvaltningen

Notat

Svar til Jakob Næsager om spørgsmål vedrørende logning af it-systemer i Københavns Kommune (KK)

15. maj 2020

Sagsnummer
2020-0115687

Dokumentnummer
2020-0115687-1

Spørgsmål
Jakob Næsager fra Det Konservative Folkeparti har på mødet i ØU den 5. maj 2020 spurgt om:

> *"Hvordan der føres kontrol med ureglementerede opslag i bl.a. CPR og andre ureglementerede opslag i kommunens systemer med personfølsomme oplysninger?"*

Besvarelse
Det lægges til grund for besvarelsen, at spørgsmålet vedrører logning og monitorering af fagsystemer i KK, som indeholder personfølsomme oplysninger.

Ansvar og kontrol

Det følger af databeskyttelsesforordningens princip om behandlingssikkerhed, at dataejer (KK) skal behandle personoplysninger, så det sikres mod uautoriseret eller ulovlig behandling og tab mv.

Af sikkerhedshensyn monitorerer kommunen egne it-systemer og brugernes anvendelse af disse. Det systemansvarlige kontor for et system er ansvarlig for, at der gennemføres periodiske logudtræk fra systemer for f.eks. at kontrollere, hvilke brugere der har adgange til data og systemet og hvilke handlinger, brugerne har udført.

Opfølgning på logning
I Københavns Kommune har man implementeret en SIEM-løsning (Security information and event management) med det formål at forbedre logning og rapportering fra fagsystemer og centrale infrastruktursystemer. SIEM er en samlet løsning, der kan benyttes til at identificere, monitorere og registrere hændelser på baggrund af de systemlogfiler, som sendes til SIEM.
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' (særlige brugsmønstre og hændelser) sendes enten regelmæssige rapporter eller specifikke alarmer til den relevante systemejer i forvaltningen, når/hvis den særlige hændelse finder sted.
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.

Koncern IT
Borups Allé 177
2400 København NV

EAN-nummer
5798009809421

www.kk.dk

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.

To eksempler

Herunder gennemgås to konkrete fagløsninger, der begge er integreret til CPR for at illustrere, hvordan logning foregår i KK.

Eksempel 1 - Automatiseret logopfølgning i CURA (elektronisk omsorgsjournalsystem i SUF)

Den væsentligste logopfølgning i CURA tager udgangspunkt i værdispringsreglen, som er hjemlet i sundhedslovens § 42 a, stk. 2. Det følger af denne bestemmelse, at sundhedspersoner ved opslag i elektroniske systemer kan indhente oplysninger om en patients helbredsforhold og andre fortrolige oplysninger, hvis indhentningen er nødvendig til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, herunder en patient, der ikke kan varetage sine interesser, sundhedspersonen eller andre. Bestemmelsen nødvendiggør, at autoriserede sundhedspersoner skal have mulighed for at tilgå oplysninger om borgerne – også uden forudgående samtykke.

For at sikre tilstrækkelige organisatoriske sikkerhedsforanstaltninger af hensyn til borgerne føres der logopfølgning med, hvor ofte medarbejdere anvender denne adgang, da muligheden er en undtagelse, der kan benyttes i særlige sager, hvis de rette juridiske betingelser er opfyldt.

Koncern IT og SUF har udarbejdet fire use cases, der via CURA automatisk alarmerer på følgende hændelser til den centrale SIEM-løsning:

1. Kontrol af hvor hyppigt værdispringsreglen anvendes for de medarbejdere, som har tilladelse til at foretage værdispring. Systemejer i SUF modtager en månedlig rapport fra SIEM.

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.

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. Systemejer i SUF modtager en daglig rapport fra SIEM.

4. Generel kontrol og statistik med alle værdispring i SUF. Systemejer i SUF modtager en månedlig rapport fra SIEM med oversigt over alle værdispring og deres fordeling på kategorierne som beskrevet ovenfor.

Eksempel 2 – Logopfølgning i eDoc (KK's elektroniske sags- og dokumenthåndteringssystem)

Den væsentlige logopfølgning i eDoc vedrører, om brugere i systemet uretmæssigt har tilgået sager med fortrolige eller personfølsomme oplysninger. ESDH-videnscenter i Koncern IT gennemfører i den forbindelse manuel logopfølgning ved løbende stikprøvekontrol med tilfældigt udvalgte brugere af systemet.

Konkret foregår logopfølgningen på den måde, at der dagligt udvælges en bruger efter et fastlagt tilfældighedsprincip, hvorefter der gennemføres kontrol med brugerens opslag i eDoc. Kontrollen fokuserer på, hvorvidt brugeren har åbnet sager eller dokumenter med følsomme værdi- eller personoplysninger, som brugeren *ikke* er sagsbehandler på. Opstår der tilfælde, hvor der kan konstateres et mistænkeligt opslag, tager ESDH videnscenter kontakt til den pågældende brugers nærmeste leder med henblik på at undersøge, om der er sket en tjenstlig forseelse.