REFERAT Direktionen d. 10-04-2024

Mødedato Onsdag d. 10. april 2024 kl. 09:00

Mødested Udvalgsværelse 1, Lemvig Rådhus

Indholdsfortegnelse

Punkt 1: Kontrol af brugeradfærd i kommunens systemer

85.15.25K08-1-24

Sagsfremstilling

Chef for Digitalisering & IT, Thomas Hyldgaard og IT-sikkerhedskonsulent & DPO, Nadia Kynde Rahbek deltager i mødet kl. 10:00.

Det er et krav til offentlige myndigheder, at der foretages løbende kontrol af medarbejderes brugeradfærd i systemer, der behandler personoplysninger. Det skal gøres for at sikre, at der ikke sker uberettiget opslag i sager, som medarbejderne ikke har et arbejdsbetinget behov for.

Det er vigtigt, at borgerne kan have tillid til, at kommunen optræder professionelt og kun tilgår de oplysninger, som de har et lovligt formål med. I den seneste tid er der set adskillige tilfælde af, at medarbejdere uberettiget har tilgået sager, som de ikke burde.

Det kan være svært at opdage uberettiget opslag, hvis medarbejdere er tildelt korrekt adgang i henhold til udførelsen af deres arbejdsopgaver. Uberettiget opslag kan derfor ikke forhindres helt, men omfanget kan forebygges ved systematisk kontrol af brugeradfærd. Systematisk kontrol kan enten gennemføres ved manuel stikprøvekontrol eller ved proaktiv logovervågning.

I Lemvig Kommune udføres opgaven i dag ikke systematisk. Der er derfor behov for, at proceduren for opgaven klarlægges. For fremadrettet at sikre systematisk kontrol i kommunen anviser Styregruppen for IT-sikkerhed nedenstående to muligheder for henholdsvis manuel stikprøvekontrol og proaktiv overvågning af brugeradfærd.

Mulighed 1: Manuel stikprøvekontrol

Manuel stikprøvekontrol indebærer, at der løbende udtrækkes en log over opslag i systemer med fortrolige og følsomme oplysninger. Kontrollen er en bagudrettet gennemgang, der foretages med skiftende intervaller eller ved mistanke. Ved denne fremgangsmåde kan der være risiko for, at en hændelse ikke identificeres rettidigt, eller slet ikke identificeres, da der kun kigges på udvalgte logdata bagudrettet.

Logudtrækket sendes til gennemgang hos medarbejderens nærmeste leder. De overordnet retningslinjer er vedlagt som bilag. Afhængigt af systemet vil det være forskelligt, hvordan loggen udtrækkes, hvilket tidsrum loggen kan trækkes for og hvor kompleks den er opbygget. Med udgangspunkt i de overordnet retningslinjer skal der derfor udarbejdes en specifik beskrivelse for loggennemgang i det pågældende system. I vedlagte retningslinjer er der lavet et eksempel på en beskrivelse specifik for systemet SAPA. Det betyder samtidig, at lederen skal forholde sig til forskellige processer i de forskellige systemer.

Pris – mulighed 1

Implementering: 0 kr.

Drift 2025: 143.083 kr.

Drift 2026: 143.083 kr.

Drift 2027: 143.083 kr.

Drift 2028: 143.083 kr.

Mulighed 2: Proaktiv overvågning via Innolog

Innolog (fra leverandøren Innofactor) er et proaktivt logovervågningssystem, som identificerer en hændelse, når den opstår. Systemet kigger på alt logdata og vil modsat en manuel stikprøvekontrol analysere data her og nu. Det er muligt at opsætte regler i Innolog, så systemet bl.a. identificerer opslag på kolleger, opslag på personer i samme husstand, opslag i egne data, opslag på familie, opslag på specifikke (kendte) personer eller sager og opslag uden for normale åbningstider

Derudover er der i Innolog mulighed for at føre stikprøvekontrol, hvor systemet udvælger tilfældige brugere til gennemgang (ligesom mulighed 1). Innolog kan også anvendes bagudrettet i forbindelse med mistanke, hvor der er muligt at se, hvor mange medarbejdere der har slået en specifik borger eller sag op, eller hvad en specifik medarbejder har slået op.

Når der implementeres systematisk og proaktiv logovervågning, bevirker det forebyggende. Det er derfor vigtigt, at det kommunikeres til medarbejdere f.eks. via ansættelsesbrevet, ledere og Intranettet.

Lederen skal løbende gennemgå og håndtere hændelser for deres medarbejdere i Innolog. Processen er strømlinet, så opgaven vil være ens for lederen, uanset hvilket system der er tilkoblet. I forbindelse med afklaring af en specifik hændelse, kan der være brug for yderligere undersøgelse i det pågældende system.

Implementering af Innolog, løbende vedligehold i Innolog, tilkobling af systemer samt vejledning og undervisning til ledere foretages af Digitalisering & IT.

Med udgangspunkt i en risikobaseret tilgang skal Innolog suppleres med manuelle stikprøvekontroller i de systemer, som ikke er tilkoblet Innolog. I disse tilfælde gælder vedlagte retningslinjer.

Pris – mulighed 2

Implementering (samlet for alle 4 år): 230.000 kr.

Drift 2025: 300.458 kr.

Drift 2026: 342.708 kr.

Drift 2027: 366.500 kr.

Drift 2028: 468.000 kr.

Tidsplanen og beregningen for de to muligheder er vedlagt i bilag 1.

Sagen afgøres endelig af

Direktionen

Lovgrundlag

Databeskyttelsesforordningens artikel 32 om behandlingssikkerhed

Økonomi

Økonomi og HR bemærker,

at der ikke kan anvises finansiering til Innolog, hvorfor en evt. godkendelse vil medføre et træk på de likvide aktiver. Finansieringen afhænger jf. ovenstående af, hvilken model/opsætning der vælges.
Ovenstående kan evt. medtages til budgetforhandlingerne for budget 2025-2028.

Indstilling
Kommunaldirektøren indstiller,

Digitaliseringsstyregruppen anbefaler,

- at systemer implementeres i Innolog over en årrække i henhold til tidsplanen i bilag 1 – ”Mulighed 2”
- at de overordnet retningslinjer for manuel stikprøvekontrol godkendes

Beslutning

Chefen for Digitalisering og IT Samt Lemvig Kommunes DPO har på mødet anbefalet en systematisk kontrol af brugeradfærden for IT-systemer, som behandler personoplysninger i overensstemmelse med Databeskyttelsesforordningen.

Direktion har besluttet at Lemvig Kommune lever op til krav om kontrol af brugeradfærd i IT systemer på en måde, der skaber begrænsede nye opgaver og begrænsede nye udgifter. Der lægges vægt på, at medarbejderne instrueres i god brugeradfærd i forbindelse med on-boarding og gennem kommunikation på intranettet, og at budskabet fremstår utvetydigt: uberettigede opslag er ulovlige og kan medføre sanktion.

Hvis der er mistankte om uhensigtmæssig brug af IT-systemer vil der bliver foretaget stikprøve kontrol af brugeradgangen til det pågældende IT-system.

Derudover foretages der rettighedsstyring af adgange til systemer samt periodisk gennemgang heraf.

Bilag

Bilag 1 - Tidsplan og beregning

Retningslinjer for kontrol af brugeradfærd i systemer med rettelser

Grundlag for kontrol af brugeradfærd

Punkt 2: Eventuelt

00.15.00I00-1-23

Beslutning

Intet

Punkt 3: Lukket: Direktionens forslag til et budget i balance 2025-2028

00.30.10P19-3-23

Punkt 4: Lukket:

00.01.00I00-2-23