REFERAT Digitaliseringsstyregruppen d. 28-02-2024

Mødedato Onsdag d. 28. februar 2024 kl. 13:00

Mødested Udvalgsværelse I

Indholdsfortegnelse

Punkt 1: IT-revision 2023

85.15.02K01-3-23

Sagsfremstilling

IT-sikkerhedskonsulent & DPO, Nadia Kynde Rahbek deltager i mødet kl. 13.00.

Som en del af den finansielle revision er der også foretaget revision af forretningsgange og kontroller inden for IT.

Revisionen omfatter Lemvig Kommunes generelle IT-kontroller, som har betydning for kommunens regnskabsføring og regnskabsaflæggelse.

Vedhæftet ledelsesbrev indeholder revisors bemærkninger og anbefalinger på de pågældende forhold.

Der er fem forhold fra tidligere, der er udbedret. Revisionens anbefalinger hertil er derfor lukket.

Derudover er (fortsat) bemærkninger på følgende tre forhold:

- Forsinket brugernedlæggelse ved medarbejderfratrædelse

- Manglende opdatering af domæne controller i perioden

- Utilstrækkelig overvågning af netværkstrafikken

Revisors bemærkninger samt Digitalisering & IT's tilhørende kommentarer gennemgås på mødet.

Bemærkningerne drøftes på baggrund af gennemgangen.

Indstilling
Chef for Digitalisering & IT indstiller,

til drøftelse

Beslutning

Drøftet

Bilag

Lemvig Kommune - IT-revisionens Ledelsesbrev 2023.pdf

Punkt 2: Kontrol af brugeradfærd i kommunens systemer

85.15.25K08-1-24

Sagsfremstilling

IT-sikkerhedskonsulent & DPO, Nadia Kynde Rahbek deltager i mødet kl. 13.00.

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.

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.

Lovgrundlag

Databeskyttelsesforordningen

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
Styregruppen for IT-sikkerhed 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

Det blev besluttet, at tydliggøre lovgivningsgrundlaget hvorefter punktet drøftes yderligere.

Bilag

Bilag 1 - Tidsplan og beregning

Retningslinjer for kontrol af brugeradfærd i systemer med rettelser

Punkt 3: Auto-complete i kommunens mailprogram

85.15.02G01-5-24

Sagsfremstilling

IT-sikkerhedskonsulent & DPO, Nadia Kynde Rahbek deltager i mødet kl. 13.00

Datatilsynet har modtaget mange indmeldelser af brud på persondatasikkerheden på grund af auto-complete i mailprogrammer. Det gør, at tilsynet har skærpet praksis i forhold til anvendelsen af auto-complete. Det er derfor ikke længere tilstrækkeligt kun at gennemføre organisatoriske foranstaltninger (f.eks. awareness) for at nedbringe risikoen for sikkerhedsbrud. Kommunen skal derfor også indføre tekniske foranstaltninger. Vurderingen skal ligeledes dokumenteres. Det gøres i en risikovurdering (vedlagt som bilag). Risikovurderingen er under udarbejdelse og vil desuden blive revurderet bl.a. i takt med ændringer i lovgivningen, eller yderligere sikkerhedsbrud i kommunen.

Beskrivelse af auto-complete

Auto-complete er en funktion, som gør, at mailprogrammet gemmer navne og mailadresser på modtagere af mails, som en medarbejder tidligere har sendt en mail til. Når en medarbejder begynder at indtaste et navn, kommer der en række forslag til modtagere. Medarbejderen kan herefter vælge en modtager fra listen. Det er muligt enten at bruge pilene og ”tab” eller musen til at vælge modtageren.

Det er tidsbesparende at anvende denne funktion og kan understøtte, at mailen fremsendes til rette modtager. Anvendelsen af auto-complete kan modsat også forårsage, at medarbejderen kommer til at vælge en forkert modtager og derfor sender mailen til uvedkommende. Hvis mailen indeholder personoplysninger, vil der være sket et brud på persondatasikkerheden.

Vurdering

Styregruppen for IT-sikkerhed har vurderet flere forskellige tekniske foranstaltninger, som alle er dokumenteret i risikovurderingen.

På baggrund af vurderingerne anbefaler Styregruppen for IT-sikkerhed at implementere følgende to tekniske foranstaltninger for at nedbringe risikoen for sikkerhedsbrud på grund af auto-complete til et acceptabelt niveau:

- Begrænsning af antal gemte mailmodtagere: der gemmes som standard 1000 mailmodtagere. Antallet nedbringes til 100. Det nedbringer konsekvensen af og sandsynligheden for et brud, da gamle mailmodtagere i højere grad sorteres fra og antallet af mulige forkerte modtagere begrænses yderligere end i dag.
- Aktivering af Mailtips: medarbejderen får en advarsel, hvis der er en ekstern modtager i modtagerlisten - uanset indholdet. Da konsekvensen vurderes størst ved fejlforsendelse til eksterne modtagere, vil en advarsel om dette nedbringe risikoen for, at der sendes mails til forkerte eksterne modtagere.

Lovgrundlag

Databeskyttelsesforordningen

Indstilling
Styregruppe for IT-sikkerhed indstiller,

- At ovennævnte to tekniske foranstaltninger implementeres

Beslutning

Digitaliseringsstyregruppen anbefaler, at de tekniske foranstaltninger implementeres.

Bilag

Risikovurdering af auto-complete (under udarbejdelse)

Punkt 4: Opfølgning på AI temadag

85.15.02G01-30-23

Sagsfremstilling

Torsdagd d. 22. februar afholdte Digitalisering og IT AI temadag for 80 deltagere fra alle områder af organisationen.

Det var en lærerig dag, hvor medarbejderne blev inspireret i forhold til, hvad kunstig intellegens herunder AI kan hjælpe med i opgaveløsningen.

Deltagerne fik en fælles viden om, hvad chatbotter kan, faldgrupperne samt Lemvig Kommunes retningslinjer.

Bilaget, AI temadag evaluering, er vedlagt.

Indstilling
Chef for Digitalisering og IT indstiller,

- punktet til orientering

Beslutning

Orientering givet.

Bilag

AI Temadag Evaluering

Punkt 5: Handleplan for digitalisering

85.13.00G01-2-23

Sagsfremstilling

Digitalisering og IT igangsatte i efteråret 23 arbejdet med en ny handleplan for digitalisering.

Handleplanen skal fastlægge rammerne for, hvordan vi implementerer strategi for digitalisering og teknologi.

Med afsæt i en modenhedsanalyse, interviews med udvalgte medarbejdere, temadag og inspiration fra andre kommuner er der udarbejdet 8 principper for digitalisering.

Principperne er retningsgivende og understøtter, hvordan vi vurderer, prioriterer, styrer og gennemfører digitaliseringsprojekter på tværs af kommunen:

1. Digitale løsninger skal forenkle og forbedre

2. Vi skaber tillid til de digitale løsninger

3. Vi sikrer bæredygtige og værdiskabende løsninger

4. Vi (gen)bruger, validerer og tilgængeliggør data

5. Vi involverer brugerne

6. Digitalisering er et fælles ansvar

7. Beslutninger tages på et ensartet og velinformeret grundlag

8. Vi samarbejder med andre og gøre brug af fælles løsninger

Der er desuden fokus på styrings-og beslutningsstrukturen, som skal sikre at digitalisering lever op til handleplanens principper; at beslutninger tages med de rette involverede og at tiltag bliver prioriteret og løst i den rette kvalitet. På mødet giver Chef for Digitalisering og IT en introduktion til tankerne om beslutningsstrukturen herunder sammensætning af digitaliseringsstyregruppen.

Indstilling
Chef for Digitalisering og IT indstiller,

- at principper for digitalisering drøftes
- at sammensætning af digitaliseringsstyregruppen drøftes

Beslutning

Punktet drøftet

Punkt 6: Lancering af nyt intranet

85.11.06P20-2-20

Sagsfremstilling

D. 29. februar lanceres det nye intranet. Formålet med et nyt intranet er at skabe en let tilgængelig, intuitiv og moderne platform til vidensdeling og samarbejde for medarbejdere i organisationen.

Der har været fokus på følgende kriterier i projektet:

- Øget selvbetjening
- Lettere at videndele og samarbejde
- Så vidt muligt at skabe en kanal til alle
- Et tidssvarende og brugervenligt design

I første implementeringsbølge har der været fokus på at kvailificere og flytte relevant indhold, ændre blanketter til formularer samt at få skabt en kanal til alle medarbejdere i kommunen. Der har desuden været fokus på at få målrettet kommunikationen, så forskellige brugerprofiler ser det der relevant for dem.

I anden bølge, som sættes igang i løbet af marts, er der fokus på selvbetjening og afdelingssider.

Der er planlagt forskellige tiltag i forbindelsen med lamceringen. Hver afdeling eller område vil få en lancerings-kurv med information. Medarbejderne vil desuden få et brev i digital post, hvor de kan læse om intranettet og hvordan man kan tilgå det fra mobile enhder. Det vil være muligt at melde sig til to webinar, hvor vi giver en rundvisning og svarer på spørgsmål og der vil komme en påskejagt.

Indstilling
Chef for Digitalisering og IT indstiller,

- punktet til orientering

Beslutning

Orientering givet.

Punkt 7: Eventuelt

85.02.02P35-77-24

Sagsfremstilling

Eventuelt

Beslutning

Der var intet under eventuelt.