TRONDHEIM KOMMUNE
Trondheim kommunerevisjon

Organisasjonsdirektør
Trude Kristin Kjelstad

Vår saksbehandler	Vår ref.	Deres ref.	Dato
Børge Sundli	22/19365 oppgis ved alle henv.		15.03.2023

Etterlevelseskontroll mot ansattilganger, systemtilganger og leverandørtilganger i Trondheim kommune - 2022

1. Innledning

Dette er en forenklet etterlevelseskontroll med økonomiforvaltningen. Kontrollen skal skje i forlengelsen av revisjonen av regnskapet og skal rette seg mot de delene av økonomiforvaltningen som går ut over å uttale seg om årsregnskapet.

Loven forutsetter at revisor gir en egen uttalelse om kontrollen som er utført. Kontrollen skal gjennomføres med såkalt moderat sikkerhet. Kravene til denne kontrollen er definert gjennom god kommunal revisjonsskikk[1] og revisjonsstandarden RSK 301 "Forenklet etterlevelseskontroll med økonomiforvaltningen". Standarden trådte i kraft fra 2020. Etterlevelseskontrollen formaliseres gjennom en uttalelse fra revisor til kontrollutvalget.

Denne etterlevelseskontrollen er rettet mot generelle IT-kontroller på økonomiområdet i Trondheim kommune. Generelle IT-kontroller er et av revisjonens årlige fokusområder. Formålet er å forebygge svakheter og bidra til å sikre at kommunen følger sentrale bestemmelser og vedtak knyttet til bruk av informasjonsteknologi på økonomiområdet.

Generelle IT-kontroller er policyer og rutiner som relaterer seg til mange IT-systemer og bidrar til å sikre kontinuerlig og hensiktsmessig drift av IT-systemene. Generelle IT-kontroller må derfor testes årlig. Valget av hva som vurderes og testes, samt omfanget av dette, vil derfor være en årlig revisjonsfaglig vurdering.

[1] Med god kommunal revisjonsskikk menes at revisjonen skal utføres i samsvar med den oppfatning av etiske og revisjonstekniske prinsipper for revisjon av kommuner som til enhver tid er alminnelig anerkjent og praktisert av dyktige og ansvarsbevisste utøvere av yrket.

Postadresse:
Trondheim kommune
Trondheim kommunerevisjon
Postboks 2300 Torgarden
7004 TRONDHEIM

Besøksadresse:
Søndre gate 10B

Telefon:
72546440

Telefaks:

Organisasjonsnummer:
NO 942 110 464

E-postadresse: revisjon.postmottak@trondheim.kommune.no
www.trondheim.kommune.no

Vi ser at den senere tids utvikling knyttet til datasikkerhet og beredskap gjør at risikobildet har endret seg, med sannsynligvis økende antall dataangrep utenfra. Ut fra en revisjonsfaglig vurdering er dette et område som må gis særskilt fokus.

Arbeidet er utført av Anne-Margit Schjølberg, Elin Ingeborg Vassmo, Elin Haarsaker og Børge Sundli.

2. Problemstilling og revisjonskriterier

I denne etterlevelseskontrollen undersøker vi om ansattilganger, systemtilganger og leverandørtilganger til IT-systemer i Trondheim kommune, kontrolleres på en tilfredsstillende måte. Vi har valgt følgende problemstilling:

1. **Har Trondheim kommune tilfredsstillende kontroll med tilganger til IT-systemene?**

Revisjonskriterier[2]

a. Kommunen skal ha retningslinjer for tilgangshåndtering til TK-nett og iT-systemer.
b. Kommunen skal etterleve retningslinjer for tilgangshåndtering.
c. Kommunen skal utføre en årlig kontroll av tilgangene til IT-systemer.
d. Kommunen skal ha kontroll og oppfølging av upersonlige tilganger.[3]
e. Kommunen skal ha kontroll og oppfølging av leverandørtilganger.[4]
f. Kommunen skal bruke sikkerhetslogger aktivt for å avdekke uønsket aktivitet i datatrafikken.

Revisjonskriteriene er utledet fra følgende kilder:

- NSM[5] Grunnprinsipper for IKT-sikkerhet
- NSM Beskytt virksomheten din mot digital utpressing
- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren punkt 5.2 Tilgangsstyring
- KS brev til kommunene - "Brev til kommunens IT-ansvarlig/IT-sikkerhetsansvarlig"
- Interna - Kvaliteket[6]: særlig:
    - ID: 16018-1, Årlig revisjon av tilganger til fagprogram med egen tilgangskontroll i Trondheim kommune
    - ID: 15741-1, IT-tilganger for ansatte og vikarer i Trondheim kommune

[2] Revisjonskriterier er de krav, normer og/eller standarder som revidert enhet skal vurderes opp mot.
[3] Upersonlig tilgang: En brukerident som ikke er knyttet til en person.
[4] Leverandørtilgang: Eksterne konsulenter og systemleverandører.
[5] NSM: Nasjonal sikkerhetsmyndighet.
[6] Kvaliteket er Trondheim kommunens kvalitetssikringssystem og består av dokumenter som prosedyrer og rutiner.

- ID: 10186-6, Bestilling av tilgang for leverandører
- ID: 1052-4, Bestilling av tilgang i LIFT for eksterne konsulenter/ ekstern attestant[7]
- ID: 16462-1, Tilgangsstyring ERP systemer
- ID: 6840-2, Retningslinjer passord

- Kjøreregler for bruk av informasjons- og kommunikasjonsteknologi (IKT) (4. januar 2023)
- Hovedrapport "Risiko- og sårbarhetsanalyse av IT-området til Trondheim kommune" 1.12.2022, unntatt offentlighet jfr Offentlighetsloven § 24 tredje ledd.

Revisjonskriteriene beskrives under hvert enkelt kapittel.

3. Metode

IT-systemer som inngår i undersøkelsen er systemer som påvirker økonomien i Trondheim kommune. IT-systemer som er valgt ut er:

- AD[8] Active Directory- autentisering- og autorisasjon av ansatte i kommunens datanettverk og tilhørende IT-systemer.
- Visma Multi -Kommunens lønns- og personalsysem.
- LIFT - Økonomisystem, kommunens regnskapssystem.
- Helseplattformen/ Epic. System for bl.a. brukerbetaling innenfor helseområdet.
- Vigilo - barnehage og SFO. System for bl.a. brukerbetaling for SFO og barnehage.
- Visma Velferd. System for administrering av økonomisk sosialhjelp.
- Komtek - Kommunale eiendomsavgifter. System for eiendomsskatt og eiendomsavgift for vann og avløp.

Metodisk baserer undersøkelsen seg på dokumentanalyse, spørreskjema og testing. Vi har undersøkt om kommunen har oppdaterte rutiner for tilgangshåndtering. Det er sendt spørreskjema til tjenesteforvaltere for de IT-systemene som inngår i denne undersøkelsen. En tjenesteforvalter er en fagperson som har ansvar for den daglige driften av et IT-system. Herunder å administrere tilganger til IT-systemet. Tjenesteforvalter er et bindeledd mellom leverandøren og kommunen. Vi har testet om tilganger som er opprettet i systemene TK-nettet, LIFT (økonomisystemet), Visma Multi (lønnsystemet) og Helseplattformen er bestilt av autorisert bestiller.

Som oppfølging av revisjonens etterlevelseskontroll fra 2021 har kommunen gjennomført en helhetlig risiko- og sårbarhetsanalyse (ROS-analyse) av IT-området. ROS-analysen ble gjennomført høsten 2022 og presentert i formannskapet 23.1.23. Saken var unntatt offentlighet, jf offentlighetsloven § 24 tredje ledd. Revisjonen har gjennomgått ROS-analysen fra 2022 og i denne rapporten har vi tatt hensyn til punkter som er aktuelle for vår problemstilling.

[7] Ekstern attestant: Eksterne konsulenter som er lagt inn i regnskapssystemet som har attestasjons- og anvisningsmyndighet.

[8] Active Directory - tilgangshånderingssystem for TK-nett.

4. Retningslinjer for tilgangshåndtering

4.1 Revisjonskriterier

Kommunen skal ha tilfredsstillende retningslinjer for tilgangshåndtering til TK-nett og IT-systemer i henhold til NSM sine grunnprinsipper[9]. Kommunen skal også ha tilfredsstillende retningslinjer for tilgangshåndtering i Helseplattformen som følger "Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren[10]". Denne normen skal blant annet sørge for at virksomheten oppretter et autorisasjonsregister.

4.2 Retningslinjer for tilgangshåndtering

Kommunen har et overordnet styringsdokument for informasjonssikkerhet, "Informasjonssikkerhetsstrategi 2021". Styringsdokumentet presiserer at informasjon som kommunen lagrer på grunnlag av sin tjenesteproduksjon og drift, utgjør store verdier. Kommunen skal sikre disse verdiene gjennom ivaretakelse av konfidensialitet, tilgjengelighet og integritet. Dette er i samsvar med krav og forventninger fra lover og forskrifter, overordnede offentlige forvaltningsmyndigheter og våre innbyggere og tjenestemottakere. Det overordnede styringsdokumentet lister blant annet opp at kommunen skal ha egne retningslinjer for tilgangskontroll, leverandørforhold og hendelseshåndtering.

I Kvaliteket er det gitt retningslinjer for tilgangshåndtering til TK-nett og IT-systemer. Ifølge retningslinjene skal det gjennomføres årlig revisjon av tilganger til fagprogram med egen tilgangskontroll. Retningslinjene beskriver hvordan IT-tilganger for ansatte og vikarer skal administreres, hvordan tilganger for leverandøren skal bestilles og hvordan tilgangsstyring i ERP[11] systemer skal håndteres.

Kvaliteket har retningslinjer, "Retningslinjer passord", som beskriver ansvar og regler for benyttelse av passord. I de samme retningslinjene er det gitt regler for bruk av midlertidig passord. Hvis den ansatte gis midlertidig passord, ved oppstart eller ved passordbytte, skal det midlertidige passordet være unikt for den ansatte og følge krav til passordkvalitet. Tjenesteforvalter for AD opplyser at det ikke lenger gis midlertidige passord til ansatte, men ansatte får beskjed om å gå til kommunens passordløsning for å resette passordet sitt. Kommunens retningslinjer er ikke oppdatert vedrørende midlertidige passord. Ved alle tilfeller hvor passordet er kjent for andre enn den ansatte selv (eksempelvis passordbytte via telefon), skal systemene tvinge den ansatte til å skifte passord ved første pålogging.

Retningslinjer for passord presiserer at ved produksjonssetting av nye IT-systemer, nye enheter og ny programvare skal alle standardpassord[12] byttes ut med unike passord som følger kravene til

---

[9] Med grunnlag i ISO 27000-serien definerer Nasjonal sikkerhetsmyndighet (NSM) et sett med grunnprinsipper og underliggende tiltak for å beskytte informasjonssystemer. Grunnprinsippene fremhever at en virksomhet må ha kontroll på hvilke rettigheter de ansatte er gitt i de IT-systemene de har tilgang til.

[10] "Ifølge "Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren" skal virksomheten sørge for at det opprettes et autorisasjonsregister.

[11] ERP: Enterprise Resource Planning - et system som bidrar til å automatisere og administrere forretningsprosesser på tvers av økonomi, produksjon, handel, forsyningskjede, personaladministrasjon og drift.

[12] Standardpassord: Forhåndssatte passord som leveres med nye IT-systemer.

passordkompleksitet.

I januar 2023 ble det via kommunens Intranett publisert "Kjøreregler for bruk av informasjons- og kommunikasjonsteknologi (IKT)". Dette er et nytt vedlegg til ansattes arbeidsavtale og opplyser om flere forhold omkring den ansattes bruk av Trondheim kommunes IKT-løsninger. Om brukeridenter og passord er følgende presisert: "*Som bruker av kommunens IT-systemer, står du personlig ansvarlig for ditt brukernavn (ident) og passord. Brukernavn og passord er svært viktig i kommunens sikkerhetsarbeid. Ditt passord er personlig og skal ikke utleveres til andre, verken i eller utenfor kommunen.*"

Fra 1.2.23 ble i tillegg regler for utforming av passord innskjerpet når det gjelder lengde på passord for kommunens datanett og kommunens administrative verktøy i Google.

Trondheim kommune benytter seg av Single Sign On (SSO)[13] for de fleste IT-systemene. Dette skjerper kravet til brukernes aktsomhet for å forhindre at uautoriserte brukere kan ta seg inn i IT-systemene. Eksempelvis er det viktig å beskytte passord, å ha generelt gode passordrutiner og låse PC/terminal når den forlates.

Tjenesteforvalter opplyser at Trondheim kommune har to-faktor autentisering aktivert på alle tjenester som er eksponert mot internett, med bruk av enten Google IdP[14] eller Azure[15] IdP. Sistnevnte er standard pålogging for kommunen framover.

4.3 ROS-analysen omtaler svakheter knyttet til tilgangshåndtering

ROS-analysen fra desember 2022 omtaler svakheter knyttet til tilgangshåndtering ved flere av kommunens IT-systemer. Det blir vist til sårbarheter knyttet til mangelfull tilgangsstyring og flere tilganger og roller enn nødvendig.

Som tiltak anbefaler ROS-analysen å etablere rollebasert tilgangsstyring og et sentralt system for å administrere ansattes brukerkontoer og tilganger på tvers av kommunens systemer. Et slikt system vil forenkle administrasjonen av de ansattes brukerkontoer og gjøre det enklere å sikre at ansatte har riktige tilganger. Det vil også kunne bidra til å fjerne tilganger når behovet opphører.

ROS-analysen omtaler også Helseplattformen hvor tilgangsstyringen ligger hos Helseplattformen AS. Det er derfor vanskelig for Trondheim kommune å få oversikt over konsekvenser hvis leverandøren gjør endringer som påvirker tilgang til systemet.

ROS-analysen anbefaler å etablere tydelig beskrivelse av roller, ansvar og myndighet for tjenesteforvalter og tjenesteeier[16]. Kommunen bør innføre formelle krav til oppgaver og ansvarsområde for tjenesteforvalter og tjenesteeier. Det bør i tillegg gjøres klart at tjenesteeier er ansvarlig for risiko knyttet til IT-systemet.

[13] SSO: Pålogging som lar en bruker få tilgang til flere applikasjoner med ett passord.

[14] IDP betyr identity provider. Det er en skybasert tjeneste som muliggjør sikker identitetsbehandling.

[15] Microsoft Azure, ofte bare kalt Azure, er en skyplattform skapt av Microsoft.

[16] Tjenesteeier: Systemeier, dette er ofte en enhet i Trondheim kommune.

ROS-analysen anbefaler å etablere retningslinjer for passord og brukernavn. I ROS-analysen anbefales det at passordretningslinjer må revideres jevnlig for å sikre at oppdaterte tekniske krav imøtekommes.

4.4 Revisjonens vurderinger

Revisjonen konstaterer at det foreligger retningslinjer i Kvaliteket for tildeling, endring og sletting av tilganger til TK-nettet og IT-systemer som kommunen administrerer tilganger for. Når det gjelder tildeling av midlertidige passord anbefaler vi at retningslinjene i Kvaliteket revideres etter dagens gjeldende rutiner.

For systemet Helseplattformen ligger tilgangsstyringen hos leverandøren Helseplattformen AS som også drifter systemet for samtlige kunder[17]. Det er laget utvidede sikkerhetstiltak for tildeling av tilganger til systemet og Trondheim kommune, har med grunnlag i en mal fra Helseplattformen AS, utarbeidet en manual for tilgangsstyring til systemet. Tjenesteforvalter opplyser at autentisering skjer i samsvar med krav i "Norm for informasjonssikkerhet i helse- og omsorgssektoren". Revisjonen ser det som positivt at Helseplattformen AS i henhold til avtale med kommunen har forpliktet seg til å følge kravene i denne normen. Vi mener det er viktig at kommunen følger opp at de får tilgangsrapporter fra Helseplattformen AS som gjør det mulig å følge opp at ansatte i Trondheim kommune har fått tilganger i henhold til tjenstlig behov.

Revisjonen støtter anbefalingene gitt i ROS-analysen om å etablere rollebasert tilgangsstyring og et sentralt system for å administrere ansattes brukerkontoer og tilganger. Det bør lages tydeligere beskrivelse av roller, ansvar og myndighet for tjenesteforvalter og tjenesteeier. Vi støtter anbefalingen i ROS-analysen om å etablere retningslinjer for passord og brukernavn. Vi ser det som positivt at kommunen har innført nye krav til lengde på passord samt at de har presisert passordreglene på kommunens interne nettsider.

5. Etterleve retningslinjer for tilgangshåndtering

5.1. Revisjonskriterier

Tilgangshåndtering til TK-nett og IT-systemer skal skje i henhold til interne retningslinjer i Kvaliteket.

5.2 Etterlevelse av retningslinjer for tilgangshåndtering

AD

Tjenesteforvalter for AD opplyser at for On-prem[18] AD benyttes kommunens retningslinjer. Tilganger styres gjennom bestillings- og slettingsrutiner, som ligger i Kvaliteket. Autorisert bestiller sender et skjema for å bestille eller slette tilganger. Slike tilganger gis i AD av IT-tjenesten. Videre oppgir tjenesteforvalter at det teknisk er sperret slik at kun den med utvidet rettigheter kan tildele disse tilgangene, samt leverandør som drifter tjenesten.

Vi fikk opplyst at gjennomgang av tilgang til AD ikke skjer så ofte fordi det er få ansatte som har utvidet tilgang, og alle disse jobber på IT-tjenesten. Når en ansatt slutter, sendes det slettemelding

[17] Samtlige kunder: St Olavs Hospital, regionale sykehus, tilknyttede kommuner i Midt-Norge, fastleger og andre private helseaktører.

[18] On-prem: betyr at programvare er installert og kjører på datamaskiner i virksomhetens eget IT-miljø.

og den ansatte slettes umiddelbart. Utvidede tilganger tildeles etter behov. Det ryddes automatisk i disse tilgangene ved at det kjøres et program som fjerner alle fra gruppa hver natt.

Tjensteforvalter opplyser at administratorer[19] må benytte Azure IdP for pålogging for å søke om utvidet tilgang, og får da tilgang for maksimalt 10 timer. Etter 10 timer forsvinner tilgangen automatisk. Dette er for å høyne sikkerheten selv om man er på innsiden av organisasjonen.

Som en del av revisjonens årlige gjennomgang av generelle IT-kontroller har vi foretatt tester av tilganger til TK-nettet og utvalgte IT-systemer. For å gjennomføre testen har vi tatt ut liste fra lønnssystemet Visma Multi over personer som hadde start- og sluttdato i kommunen i 2022. I denne kontrollen ønsket vi å få dokumentasjon på at bestillingsskjema for IT-tilganger er kommet fra autorisert bestiller og se at bestillingen er registrert i AD. Alle tilganger som er kontrollert er bestilt av autorisert bestiller. Revisjonens test viser at alle som er kontrollert har fått riktig tilgang i økonomisystemet LIFT og lønnssystemet Visma Multi.

Visma Multi - Lønns- og personalsystem
Tjenesteforvalter viser til de generelle retningslinjene i kommunen og viser til at det er opprettet en egen rutine for tilgangshåndtering for ERP systemene[20] som IT-tjenesten håndterer. Dette gjelder også for utvidede tilganger i Visma Multi for ansatte som skal kunne hente fra eller sende data til offentlige registre som Folkeregister, Altinn og AA registeret[21]. Ifølge tjenesteforvalter er disse registrene viktige for å utføre oppgaver på lønnsområdet.

LIFT
Tjenesteforvalter for LIFT opplyser at kommunens overordnede styringsdokumenter blir lagt til grunn for tilgangshåndtering. På samme måte som for Visma Multi viser de til at det er en egen rutine for tilgangshåndtering for ERP-systemene som IT-tjenesten håndterer.

Enheter i Trondheim kommune som skal gi eksterne prosjektledere tilganger til LIFT, må følge rutinen "Bestilling av tilgang for leverandører" i Kvaliteket.

Helseplattformen/Epic
Det er utarbeidet en manual for tilgangsstyring i Helseplattformen for Trondheim kommune. Avtalen mellom Trondheim kommune og Helseplattformen," Bilag 7 Behandling av personopplysninger", forplikter at autentisering til Helseplattformen skal skje i samsvar med krav oppstilt i "Norm for informasjonssikkerhet i helse- og omsorgssektoren".

Revisjonen er informert om at tilgang til systemet kan gis på to måter, via funksjonskode (stilling) eller via bestilling fra autorisert bestiller. For å logge inn i Helseplattformen kreves det identifisering på sikkerhetsnivå fire; det vil si med nøkkelbrikke, BankID eller smartkort (med kvalifisert sertifikat). Trondheim kommune har valgt nøkkelbrikken som standard metode.

Helseplattformen ble tatt i bruk av kommunen i 2022. Dette systemet inneholder mye sensitive personopplysninger for kommunens innbyggere. Revisjonen har derfor gjennomført tester av tilganger til systemet. Vi har kontrollert om tilganger til systemet er gitt i henhold til kommunens

[19] Administrator: Ansatt med utvidede rettigheter i IT-systemer.

[20] ERP systemene: Fagsystemene LIFT (økonomi) og Visma Multi (lønn og HR).

[21] AA-registeret: Arbeidsgiver- og arbeidstakerregisteret.

retningslinjer og er bestilt av autorisert bestiller. Det forelå ikke bestillingsskjema for flere av de tilgangene som ble kontrollert, men e-poster fra autorisert bestillere ble brukt som dokumentasjon.

Tjenesteforvalter opplyser i dialog med revisjonen at mappingreglene[22] knyttet til enhet og funksjon er kvalitetssikret av innføringsprosjektet. Tjenesteforvalter uttaler at tilganger utover mappingreglene bestilles av autorisert bestiller via Service Now[23]. Etter at St Olavs hospital innførte Helseplattformen, 12. november 2022, opplyser tjenesteforvalter at tilgangsstyringssystemet er stabilt.

Vigilo
Tjenesteforvalter opplyser at de følger rutiner i kvaliteket for tilgangshåndtering for Vigilo. Pålogging for kommunalt ansatte er basert på Azure AD[24] og styres av en egen tilgangsgruppe der. Den inneholder alle ansatte fra skoler og barnehager. For private barnehager skjer pålogging ved hjelp av ID-porten. Tjenesteforvalter opplyser også at de tildeler roller basert på det behovet den enkelte ansatte har, kombinert med Vigilo sin beskrivelse av de ulike rollene.

Visma Velferd
Tjenesteforvalter opplyser at enheten foretar bestilling til kommunens AD administrasjon som sendes videre til de som håndterer fagprogrammet i henhold til kommunens rutine. De kontrollerer at bestilling er slik de forventer for den ansatte og gir rolletilganger. I tillegg utformes det en delegasjonsavtale mellom leder og ansatt som angir type vedtak som kan fattes av den enkelte. Systemet er satt opp slik at det skal være to personer som behandler vedtak om utbetalinger.

Komtek
Tjenesteforvalter opplyser at de benytter skriftlige rutiner i Kvaliteket "Tilgangsstyring for IT-systemer". Installasjonen av systemet gjøres på grunnlag av medlemskap i egne AD-grupper for Komtek og bestilles av enhetenes autoriserte bestiller.

Tjenesteforvalteren gir uttrykk for at dette er et lite fagfelt og det er få som jobber med Komtek. Komtek er et så gammelt system at det ikke tar imot AD-grupper[25] for autorisasjon. De får derfor i stedet e-poster med forespørsel om brukere til systemet. Nye brukere må legges inn manuelt av tjenesteforvalter.

Historikken i Komtek er knyttet til ansattes brukerkontoer. De kan derfor ikke fjerne brukerkontoene til ansatte som slutter eller ikke lenger skal ha tilgang til systemet. Dersom ansatte fjernes fra Komtek, forsvinner ikke loggen fysisk, men de vet ikke hvem loggen tilhører. Loggene fra Komtek må tas vare på fram til det kommer en ny omtaksering av eiendommene. Omtakseringsperiodene varer i 10 til 15 år.

[22] Mappingreglene: Regler for tilgang til Helseplattformen ut fra hvilken funksjon de ansatte har og hvor de jobber.

[23] Service Now: Verktøy som benyttes av Trondheim kommune for digitalisering og automatisering av prosesser.

[24] Azure AD: Et system i Microsoft Azure som muliggjør identitetshåndtering for å konfigurere tilgang til tjenester og ressurser for brukere og grupper.

[25] AD-gruppe: En gruppe som inneholder flere brukerkontoer. Rettigheter, tilganger og begrensninger er likt for alle brukerkontoene som er medlem av gruppa.

5.3 Revisjonens vurdering

Tjenesteforvalterne for IT-systemene som inngår i undersøkelsen, bekrefter at kommunens retningslinjer benyttes.

Revisjonens tester av tilganger til TK-nettet og systemene LIFT og Visma Multi bekrefter at bestilling er utført av autorisert bestiller.

Revisjonens tester av tilganger til systemet Helseplattformen viser at tilganger var bestilt av autorisert bestiller, men e-poster ble brukt i stedet for bestillingsskjema. Tjenesteforvalter opplyser at dette skyldes innkjøringsproblemer i oppstartsfase, men at tilgangsstyringssystemet nå er stabilt. Revisjonen mener det er svært viktig at bestilling av tilganger til systemet Helseplattformen blir gjort i henhold til gjeldende retningslinjer.

6. Årlig kontroll av tilgangene til IT-systemer

6.1. Revisjonskriterier

Tjenesteforvalterne skal minimum en gang per år ta ut oversikt over brukere av fagprogram og gjennomføre en kontroll av hvem som har tilgang til IT-systemet i henhold til rutine i Kvaliteket[26]. Denne oversikten skal sendes til aktuelle enheter på e-post. Enhetene skal gjennomgå den mottatte oversikten og sende bestilling på sletting av tilgang for de som ikke lengre skal ha denne.

6.2 Krav til årlig kontroll av tilganger

Tjenesteforvalterne har svart på dette i spørreundersøkelsen.

AD

Tjenesteforvalter svarer at det i AD utføres en obligatorisk gjennomgang av de med utvidede tilganger en gang i året.

Visma Multi - Lønns- og personalsystem

Tjenesteforvalter svarer at de ikke utfører en årlig gjennomgang av tilganger. Systemet har en rapport "Roller og tilganger" som kan benyttes til en slik kontroll. Det er ikke distribuert rapporter til ledere/autoriserte bestillere, med oversikt over ansatte og tilganger/roller i HR-Portalen.

LIFT

Tjenesteforvalter opplyser at det ikke gjennomføres årlig gjennomgang av tilganger til systemet, men det planlegges å etablere en rapport som skal sendes enhetene i kommunen for gjennomgang.

Tjenesteforvalter anbefaler i dag autoriserte bestillere/ledere på enhetene å bruke eksisterende rapporter i LIFT.

Helseplattformen/Epic

Tjenesteforvalter opplyser at det i utgangspunktet er HR-portalen[27] som styrer tilgangene til

[26] Årlig revisjon av tilganger til fagprogram med egen tilgangskontroll i Trondheim kommune.

[27] HR-portal: Den delen av lønns- og personalsystemet som ansatte og enheter daglig benytter.

Helseplattformen. Det er enhetslederne som har et ansvar for å melde ansatte riktig inn i HR-portalen. Vi har fått opplyst at det derfor ikke er planlagt noen årlig og sentral gjennomgang av tilganger til Helseplattformen.

Vigilo
Tjenesteforvalter opplyser at det ikke er gjennomført noen årlig revisjoner av tilganger så langt. De vil fra nå av hente ut lister over de opprettede brukerne på hver enkelt enhet og sende disse ut for revisjon i forbindelse med oppstarten av nytt skole- og SFO-år.

Visma Velferd
Tjenesteforvalter opplyser at det kjøres ut lister som viser hvilke ansatte som har tilgang til systemet. Listene er grunnlag for NAV-enhetene som sjekker om tilgangene er riktige, og som melder ut de ansatte som ikke har behov for tilgang eller har sluttet. Tjenesteforvalter har ikke tatt vare på dokumentasjon av gjennomføringen.

Komtek
Tjenesteforvalter opplyser at det gjøres en årlig gjennomgang av tilganger. Ansattes brukerkontoer fjernes ikke, men man deaktiverer dem for å beholde loggen i Komtek. Historikken i Komtek er knyttet til ansattes brukerkontoer. De kan derfor ikke fjerne brukerkontoer for da forsvinner historikken. Videre oppgir tjenesteforvalter at loggen ikke forsvinner fysisk, men de vet ikke hvem loggen tilhører dersom ansattes brukerkontoer blir fjernet.

6.3 Revisjonens vurderinger
Undersøkelsen viser at det mangler årlig gjennomgang av tilganger ved flere av IT-systemene som er kontrollert i undersøkelsen. Revisjonen mener at årlig gjennomgang bør gjennomføres i henhold til retningslinjene i kommunen.

7. Kontroll av upersonlige tilganger

7.1 Revisjonskriterier
Kommunen skal ha kontroll av upersonlige tilganger i henhold til NSM Grunnprinsipper for IKT-sikkerhet[28] og kommunens retningslinjer[29] for bruk av passord.

7.2 Kontroll av upersonlige tilganger
AD
Ifølge tjenesteforvalter tar de utgangspunkt i at en upersonlig tilgang oppfattes som tjenestekonto der en tjeneste skal autentisere seg overfor AD. De aller fleste tjenestekontoer[30]er såkalt beskyttet tjenestekonto. For disse kontoene har man ekstra kontroll slik at man ikke kan gjøre endringer på kontoene. Tjenesteforvalter oppgir at slike kontoer bestilles av et prosjekt ved en anskaffelse eller etablering av en tjeneste, der det opprettes en "beskyttet tjenestekonto". Slike kontoer har den mest kompliserte passordpolicyen og det kreves at tjenesteforvalter bestiller sletting av kontoer når tilhørende tjeneste opphører. Dette sikres ved at leverandøren er ansvarlig for å slette

[28] Punkt 2.0- 2.6. omhandler kontroll av identer og tilganger.

[29] Retningslinjer for passord i Kvaliteket omhandler behandling av midlertidige passord og forhåndssatte passord.

[30] Tjenestekonto: Bruker-ID som ikke er knyttet til en person.

tjenestekonto knyttet til tjenesten som er bestilt avviklet.

Visma Multi - Lønns- og personalsystem
Tjenesteforvalter opplyser at Trondheim kommune ikke har spesifikke krav til oppfølging av upersonlige tilganger. Det er leverandøren av tjenesten som initierer behov for slike tilganger, for eksempel arbeidsflyt i skjema (robot) og ved kjøring av systemtekniske jobber.

LIFT
Tjenesteforvalter opplyser at kommunen ikke har noen spesifikke krav til oppfølging av upersonlige tilganger. Det er leverandøren som initierer behov for slike tilganger, for eksempel arbeidsflyt og kjøring av systemtekniske jobber. Det gjøres noen kontroller av oppfølging av upersonlige tilganger, men kontrollene utføres ikke i henhold til en plan.

Helseplattformen/Epic
Tjenesteforvalter opplyser at Helseplattformen AS styrer tilganger. Tjenesteforvalter er ikke kjent med at det foreligger upersonlige tilganger for Trondheim kommune.

Vigilo
Tjenesteforvalter svarer at upersonlige tilganger opprettes med svært begrensede rettigheter, og benyttes i det daglige av ansatte ved SFO eller barnehage. Disse benyttes på flerbrukerutstyr som PC-er, nettbrett eller smarttelefon, for å forenkle registrering av barn ved levering og henting i barnehage og SFO. Upersonlige tilganger tildeles kun rollen "Begrenset bruker". Rollen "Begrenset bruker" har ikke tilgang til personopplysninger. Leverandøren har ingen upersonlige tilganger til Trondheim kommunes installasjon av løsningen.

Visma Velferd
Tjenesteforvalter opplyser at det kun er driftspersonell hos driftsleverandør, Sopra Steria[31] eller systemleverandør Visma, som har tilgang via upersonlige tilganger. Formkravene til dette og løsningen er utarbeidet av IT-tjenesten. Teknisk personell får i samarbeide med leverandøren tildelt tilganger.

Komtek
Tjenesteforvalter opplyser at upersonlige tilganger tildeles kun når leverandør skal ha tilgang for å utføre en aktivitet som er bestilt av Trondheim kommune. Det er på svartidspunktet ikke bruk av upersonlige tilganger til Komtek.

7.3 Revisjonens vurdering
Tjenesteforvalter for AD opplyser at der er god kontroll på upersonlige tilganger.

Tjenesteforvaltere for skysystemene Visma Multi og LIFT opplyser at Trondheim kommune ikke har spesifikke krav til oppfølging av upersonlige tilganger. De sier at det er leverandøren av tjenesten som initierer behov for slike tilganger.

For systemer som driftes lokalt hos Sopra Steria, som Visma Velferd og Komtek, har tjenesteforvalterne kontroll med upersonlige identer som gis tilgang til IT-systemene.

[31] Sopra Steria: Trondheim kommunes driftsleverandør for drift av "Lokale IT-systemer".

Tjenesteforvalter for Vigilo svarer at upersonlige tilganger opprettes med svært begrensede rettigheter, og benyttes i det daglige av ansatte ved SFO eller barnehage.

Revisjonen mener det bør utarbeides spesifikke retningslinjer for oppfølging av upersonlige brukeridenter. Trondheim kommune må stille krav til at leverandørene følger kommunens retningslinjer og at det rapporteres til kommunen på håndtering av upersonlige tilganger. Kommunen bør ha en årlig gjennomgang av behovet for de upersonlige tilgangene.

8. Kontroll av leverandørtilganger

8.1 Revisjonskriterier

Kommunen skal ha kontroll og oppfølging av leverandørtilganger i henhold til NSM Grunnprinsipper for IKT-sikkerhet[32] og kommunens retningslinjer[33] for tilgangshåndtering.

8.2 Kontroll av leverandørtilganger

AD

Trondheim kommune har innført en ny løsning for leverandørtilgang kalt PAM[34] (Privileged Access Management). Ifølge tjenesteforvalter forenkler dette administrasjon av leverandørtilganger. Når det kommer en bestilling av en leverandørtilgang, skal det avklares og innhentes nødvendig informasjon om behovet for tilgangen. Etter at tilgangen er opprettet skal tjenesteforvalter, som kjenner tjenesteleverandøren, invitere brukere som skal ha tilgang til applikasjonen. Dette skjer ved å sende en unik lenke til leverandøren med invitasjon til kommunens Azure AD[35], der vedkommende får opprettet en gjestekonto. Når leverandørbrukeren har behov for tilgang til TK-nettet, søker han om tilgang som blir godkjent av tjenesteforvalter eller Incident manager[36], avhengig av hvilke type aktivitet det er snakk om. Det blir opprettet tilgangsstyringspakker[37] som gir 24 timer, sju dager eller maksimalt 365 dager tilgang.

Tjenesteforvalter opplyser at ansatte fra leverandørene Tieto EVRY og Unit4 som skal jobbe i LIFT Web-løsning[38], må ha kommunal Azure AD konto. Det må underskrives avtale med leverandøren om tildeling og bruk av kommunal Azure AD konto. Hver nye leverandørbruker må underskrive taushetserklæring, som er utarbeidet av Trondheim kommune og oppbevares hos leverandøren. Ved bestilling av tilgang skal leverandøren bekrefte at taushetserklæringen er signert.

Tjenesteforvalter opplyser at når en leverandørbruker slutter hos leverandøren, blir brukerkontoen hos leverandøren satt ut av funksjon og slettet. Etterpå blir brukerkontoen satt ut av funksjon i Trondheim kommunes Azure AD.

---

[32] Punkt 2.0- 2.6. omhandler kontroll av identer og tilganger.

[33] I kvaliteket foreligger en retningslinje "Bestilling av tilgang i LIFT for eksterne konsulenter/ ekstern attestant.

[34] PAM: Privileged Access Management (PAM) er en identitetssikkerhetsløsning som bidrar til å beskytte organisasjoner mot cybertrusler ved å overvåke, oppdage og forhindre uautorisert privilegert tilgang til kritiske ressurser.

[35] Azure AD: Et system i Microsoft Azure som muliggjør identitetshåndtering for å konfigurere tilgang til tjenester og ressurser for brukere og grupper.

[36]Incident manager: Ansatt med ansvar for hendelsesstyring.

[37] Tilgangsstyringspakker: Gir leverandøren tilgang i et definert tidsrom.

[38] LIFT Web-løsning: Trondheim kommunes WEB-basert portal mot økonomisystemet - Unit4.

Visma Multi - Lønns- og personalsystem
Tjenesteforvalter opplyser at avtalen med Visma krever at leverandøren skal dokumentere tilganger. Ifølge tjenesteforvalter bestilles rapport over leverandørtilganger cirka to ganger per år, og Trondheim kommune som kunde og leverandøren tar en felles gjennomgang på statusen.

Visma som leverandør gir sine ansatte tilganger i HR-Portal og Visma Multi Ekspert[39]. De oppgir at de retter seg etter punkt om sikkerhet i databehandleravtalen[40].

LIFT
Tjenesteforvalter svarer at de kontroller tilganger for prosjektledere (eksterne attestanter) halvårlig. Revisjonen har i tidligere undersøkelser sett at det er til dels mange ansatte hos leverandøren som har tilgang til systemet. Vi har fått opplyst at det gjennomføres regelmessige gjennomganger av identene.

Helseplattformen/Epic
Helseplattformen AS, som drifter systemet, gir sine ansatte tilganger til systemet. Hemit HF[41] drifter serverne som Helseplattformen kjøres på. Tjenesteforvalter sier at løsningsarkitekter hos Helseplattformen AS logger seg på med sin bruker og kan ta over hvilken som helst bruker i Trondheim kommune. Denne aktiviteten logges.

Vigilo
Tjenesteforvalter opplyser at de personene som er gitt tilgang fra leverandør er avtalt mellom l tjenesteforvalter og tjenesteeier i kommunen og leverandørens prosjektleder.

Visma Velferd
Tjenesteforvalter oppgir at formkravene til oppfølging av leverandørtilganger er utarbeidet av IT-tjenesten. Teknisk personell får i samarbeid med leverandøren tildelt azure-tilganger. De må godkjennes for hvert oppdrag, hvor tjenesteforvalter godkjenner tilgangen.

Komtek
Tjenesteforvalter opplyser at systemleverandøren beskriver tilgangshåndteringen i driftsavtalen og databehandleravtalen de har med kommunen. Leverandøren har ingen fast tilgang til Komtek, men tilgang til systemet gis enkeltvis og det styres av Trondheim kommune ved tjenesteforvalter for Komtek.

8.3 ROS-analysen knyttet til leverandørtilganger
ROS-analysen anbefaler å etablere standardkontrakter og gode rutiner for kommunikasjon med leverandør. Det nevnes at Trondheim kommune må stille sikkerhetskrav til sine leverandører som tar for seg blant annet rutine for sikkerhet og bruk av informasjon.

[39] Visma Multi Ekspert: Visma Multi inneholder en egen ekspertmodul for lønnsmedarbeidere. Herfra håndteres alt som omfatter lønn, lønnsutbetaling og innrapportering.

[40] Databehandleravtalen skal sikre at personopplysningene blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysningene.

[41] Hemit HF: Er et helseforetak stiftet i 2021. Det eies av Helse Midt-Norge RHF. Helseforetaket har ansvar for sentral drift og forvaltning av felles IKT-systemer for alle sykehus i helseregionen.

8.4 Revisjonens vurdering

Undersøkelsen viser at Trondheim kommune mangler gode rutiner for oppfølging av leverandørtilganger for systemleverandør. Revisjonen er enig med ROS-analysen sine anbefalinger om å etablere standardkontrakter og gode rutiner for kommunikasjon med leverandør. Dette kan bidra til en målrettet oppfølging av leverandørtilganger.

9. Sikkerhetslogger

9.1 Revisjonskriterier

Kommunen skal bruke sikkerhetslogger aktivt for å avdekke uønsket aktivitet i datatrafikken i henhold til NSM grunnprinsipper punkt 4.3.

9.2 Bruk av sikkerhetslogger for å avdekke uønsket aktivitet i datatrafikken

AD

Tjenesteforvalter opplyser at det gjøres nødvendig sikkerhetslogging i AD. Blant annet logges vellykket innlogging og utlogging. Under "applikasjonslogger"[42] loggføres feil som oppstår og informasjon som er nødvendig for drift av AD. Det utføres også en kontinuerlig systemlogg for hendelser i systemet, samt informasjon om forsøk fra andre systemer på å logge seg på AD. Logger fra AD videresendes til Microsoft Azure Sentinel[43] for analyse og eventuell oppfølging.

Visma Multi - Lønns- og personalsystem

Tjenesteforvalter uttaler at logger ikke benyttes aktivt, men at det er logger som kan benyttes hvis man har mistanke om uønsket aktivitet - eller det oppstår feilsituasjoner. Alt sikkerhetslogges i systemet, men det må spesifiseres overfor leverandør hvilke opplysninger man ønsker å få listet ut fra loggen.

LIFT

Tjenesteforvalter opplyser at siden innføringen av LIFT har leverandørens anbefalinger for logging av endringer vært skrudd på. Disse loggene kan analyseres ved feilsituasjoner og mistanke om uønsket aktivitet.

Helseplattformen/Epic

Tjenesteforvalter sier at de jobber med å utarbeide gode rapporter for å analysere logger. Målet er ifølge tjenesteforvalter å etablere en rutine som avdekker om uautoriserte har forsøkt å få tilgang til opplysninger. Rapporten vil vise om forsøkene på tilgang er avvist eller hvilken begrunnelse som er benyttet for å få tilgang i de ulike situasjonene.

Ifølge tjenesteforvalter kontrollerer de hvem som har hatt oppslag i journalene for konfidensielle brukere. Det avdekkes om eventuelt uautoriserte har kommet inn/forsøkt å komme inn i disse journalene. Tjenesteforvalter opplyser at denne rapporten så langt er levert etter forespørsel.

[42] En applikasjonslogg er en fil med hendelser som er logget av et program. Den inneholder feil, informasjonshendelser og advarsler.

[43] Microsoft Azure Sentinel er en skybasert tjeneste som tilbyr intelligente sikkerhetsanalyser drevet av kunstig intelligens.

Vigilo
Tjenesteforvalter opplyser at siden dette er en skytjeneste[44] er det leverandøren som logger uønsket trafikk fra utsiden, og ivaretar det sikkerhetsmessige der. All aktivitet logges i systemet, og aktivitet kan ettergås med bistand fra leverandør.

Visma Velferd
Tjenesteforvalter svarer at de ikke kjenner til dette.

Komtek
Ifølge tjenesteforvalter kjøres Komtek på serverparken hos Sopra Steria som melder fra hvis det er uønsket aktivitet i Komtek.

9.3 ROS-analyse knyttet til sikkerhetslogger
ROS-analysen fra desember 2022 anbefaler innføring av sikkerhetslogging i alle systemer og at det etableres sikkerhetsovervåking. ROS-analysen beskriver at sikkerhetslogging bør være konfigurert slik at kommunen raskt kan håndtere hendelser.

9.4 Revisjonens vurdering
Revisjonens undersøkelse viser at det er svakheter knyttet til sikkerhetslogging og sikkerhetsovervåking for kommunens IT-systemer. Revisjonen slutter seg til ROS-analysens anbefalinger om å innføre sikkerhetslogging i alle systemer og etablere sikkerhetsovervåking. Hvis det oppstår en alvorlig hendelse, må sikkerhetsloggingen være konfiguert slik at Trondheim kommune raskt kan reagere og håndtere situasjonen.

10. Konklusjon

Kommunen skal ha retningslinjer for tilgangshåndtering til TK-nett og iT-systemer
Undersøkelsen viser at det foreligger retningslinjer for tildeling, endring og sletting av tilganger til TK-nettet og IT-systemer. Retningslinjene for tildeling av midlertidige passord samsvarer ikke med dagens praksis. Retningslinjene bør oppdateres.

Gjennomført undersøkelse viser at autentisering til Helseplattformen skjer i samsvar med krav i "Norm for informasjonssikkerhet i helse- og omsorgssektoren". Revisjonen mener imidlertid det er viktig at kommunen følger opp at de får tilgangsrapporter fra Helseplattformen AS som gjør det mulig å følge opp at ansatte i Trondheim kommune har fått tilganger i henhold til tjenstlig behov.

Revisjonen støtter anbefalingene gitt i ROS-analysen om å etablere rollebasert tilgangsstyring og et sentralt system for å administrere ansattes brukerkontoer og tilganger. Det bør lages tydeligere beskrivelse av roller, ansvar og myndighet for tjenesteforvalter og tjenesteeier. Vi støtter anbefalingen i ROS-analysen om å etablere retningslinjer for passord og brukernavn.

[44] Skytjenester er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett.

Kommunen skal etterleve retningslinjer for tilgangshåndtering

Kommunens retningslinjer for tilgangshåndtering benyttes for IT-systemene som inngår i undersøkelsen. For systemet Helseplattformen har det vært innkjøringsproblemer i oppstartsfasen, men tilgangsstyringssystemet er nå stabilt. Revisjonen mener det er svært viktig at bestilling av tilganger til systemet Helseplattformen blir gjort i henhold til gjeldende retningslinjer.

Kommunen skal utføre en årlig kontroll av tilgangene til IT-systemer

Det mangler årlig gjennomgang av tilganger ved flere av IT-systemene som er kontrollert i undersøkelsen. Revisjonen mener at årlig gjennomgang bør gjennomføres i henhold til retningslinjene i kommunen.

Kommunen skal ha kontroll og oppfølging av upersonlige tilganger

Gjennomført undersøkelse viser at for systemer som driftes lokalt hos Sopra Steria har kommunen kontroll med upersonlige identer. For skysystemene Visma Multi og LIFT er det ikke satt spesifikke krav til oppfølging av upersonlige tilganger. Det er leverandøren av tjenesten som initierer behov for slike tilganger.

Revisjonen mener det bør utarbeides spesifikke retningslinjer for oppfølging av upersonlige brukeridenter. Det må stilles krav til at leverandørene følger kommunens retningslinjer og at det rapporteres på håndtering av upersonlige tilganger. Kommunen bør også ha en årlig gjennomgang av behovet for de upersonlige tilgangene.

Kommune skal ha kontroll og oppfølging av leverandørtilganger

Undersøkelsen viser at Trondheim kommune mangler gode rutiner for oppfølging av leverandørtilganger for systemleverandør. Revisjonen er enig med ROS-analysen sine anbefalinger om å etablere standardkontrakter og gode rutiner for kommunikasjon med leverandør.

Kommunen skal bruke sikkerhetslogger aktivt for å avdekke uønsket aktivitet i datatrafikken

Gjennomført undersøkelse viser at det er svakheter knyttet til sikkerhetslogging og sikkerhetsovervåking for kommunens IT-systemer. Revisjonen slutter seg til ROS-analysens anbefalinger om å innføre sikkerhetslogging i alle systemer og etablere sikkerhetsovervåking.

11. Tilsvar på rapporten

Vi ber om svar innen 30. mars 2023. Revisoruttalelsen skal etter planen til behandling i kontrollutvalget 8. mai 2023.

Med hilsen

Per Olav Nilsen
revisjonsdirektør

Børge Sundli
revisor/CISA

Elektronisk dokumentert godkjenning uten underskrift

Kopimottaker: Postmottak Organisasjonsdirektøren, Organisasjonsdirektøren