TRONDHEIM KOMMUNE
Trondheim kommunerevisjon

Kontrollutvalget

Vår saksbehandler	Vår ref.	Deres ref.	Dato
Børge Sundli	22/19365 oppgis ved alle henv.		19.04.2023

Uavhengig revisors attestasjonsuttalelse om "Etterlevelseskontroll mot ansattilganger, systemtilganger og leverandørtilganger i Trondheim kommune - 2022"

Vi har utført et attestasjonsoppdrag som skal gi moderat sikkerhet, i forbindelse med Trondheim kommunes etterlevelse av bestemmelser knyttet til IT-sikkerhet.

Problemstilling
Har Trondheim kommune tilfredsstillende kontroll med tilganger til IT-systemene?

Kriteriene har vært at kommunen skal:

- ha retningslinjer for tilgangshåndtering til TK-nett og IT-systemer
- etterleve retningslinjer for tilgangshåndtering
- utføre en årlig kontroll av tilgangene til IT-systemer
- ha kontroll og oppfølging av upersonlige tilganger
- ha kontroll og oppfølging av leverandørtilganger
- bruke sikkerhetslogger aktivt for å avdekke uønsket aktivitet i datatrafikken

Revisjonskriterier er utledet fra følgende kilder:

- NSM[1] 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"
- Aktuelle interne rutiner knyttet til IT-området
- Hovedrapport "Risiko- og sårbarhetsanalyse av IT-området til Trondheim kommune" 1.12.2022, unntatt offentlighet jfr Offentlighetsloven § 24 tredje ledd.

Ledelsens ansvar for etterlevelse av bestemmelser og vedtak for økonomiforvaltningen
Kommunedirektøren er ansvarlig for å etablere administrative rutiner som sørger for at

[1] NSM: Nasjonal sikkerhetsmyndighet.

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

økonomiforvaltningen utøves i tråd med bestemmelser og vedtak, og at økonomiforvaltningen er gjenstand for betryggende kontroll.

Vår uavhengighet og kvalitetskontroll
Vi har utført oppdraget i samsvar med etiske retningslinjer for kommunerevisjonen, som inneholder uavhengighetskrav og andre krav basert på grunnleggende prinsipper om integritet, objektivitet, faglig kompetanse og tilbørlig aktsomhet, fortrolighet og profesjonell opptreden. I samsvar med internasjonal standard for kvalitetsstyring (ISQM 1 Kvalitetsstyring for revisjonsforetak som utfører revisjon eller forenklet revisorkontroll av regnskaper, eller andre attestasjonsoppdrag eller beslektede tjenester") har Trondheim kommunerevisjon et tilstrekkelig kvalitetskontrollsystem, herunder dokumenterte retningslinjer og rutiner for etterlevelse av etiske krav, faglige standarder og krav i gjeldende lovgivning og annen regulering.

Våre oppgaver og plikter
Vår oppgave er å avgi en uttalelse om etterlevelse av bestemmelser og vedtak for økonomiforvaltningen på grunnlag av bevisene vi har hentet inn. Vi har utført vårt attestasjonsoppdrag med moderat sikkerhet i samsvar med kommunelovens regler og RSK 301 Forenklet etterlevelseskontroll med økonomiforvaltningen. Standarden krever at vi planlegger og gjennomfører oppdraget for å oppnå moderat sikkerhet for hvorvidt det foreligger vesentlige feil eller mangler ved etterlevelse av bestemmelser og vedtak i kommunens økonomiforvaltning på det området vi har foretatt forenklet etterlevelseskontroll.

Vi baserer oppgaven på en risiko- og vesentlighetsvurdering.

Utføring av et attestasjonsoppdrag som skal gi moderat sikkerhet i henhold til RSK 301, innebærer å utføre handlinger for å innhente bevis for at bestemmelser og vedtak for økonomiforvaltningen etterleves. Typen, tidspunktet for og omfanget av de valgte handlingene er gjenstand for revisors skjønn. Moderat sikkerhet har klart lavere sikkerhetsgrad enn betryggende sikkerhet, og vi gir derfor ikke uttrykk for samme nivå av sikkerhet som i en revisjonsberetning.

Vi mener at vi har innhentet tilstrekkelig og hensiktsmessig bevis som grunnlag for vår konklusjon.

Grunnlag for konklusjon
Vi viser til vårt brev til organisasjonsdirektøren av 15. mars 2023 og tilsvar av 14. april 2023.

Nedenfor gjengis revisjonens anbefalinger i brevet med svarene fra administrasjonen:

- Retningslinjene for tildeling av midlertidige passord samsvarer ikke med dagens praksis. Retningslinjene bør oppdateres. Revisjonen 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. Det bør lages tydeligere beskrivelse av roller, ansvar og myndighet for tjenesteforvalter og tjenesteeier.

  Svar: Retningslinjer for midlertidige passord er nå oppdatert i aktuell rutine i Kvaliteket Tilgangsrapporter fra Helseplattformen skal nå jevnlig etterspørres. Arbeidet med å oppdatere rollebeskrivelser er igangsatt som del av en gjennomgang av hvordan Trondheim kommune utøver IT tjenestestyring.

- Revisjonen mener det er svært viktig at bestilling av tilganger til systemet Helseplattformen blir gjort i henhold til gjeldende retningslinjer.

  Svar: Bestilling av tilganger til systemet Helseplattformen blir nå gjort i henhold til gjeldende retningslinjer. De refererte innkjøringsproblemene på dette området er nå over.

- 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.

  Svar: Dette erkjenner vi at er et område hvor vi må legge ned mer innsats og tilstrebe at dette gjøres for alle systemene hvert år.

- 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. 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.

  Svar: Vi erkjenner at vi må kravstille at våre leverandører håndterer denne typen tilganger på en god måte, men vi vil sannsynligvis ikke være i stand til å kreve at leverandørene tilpasser intern praksis iht våre retningslinjer fullt ut. Dette som en naturlig konsekvens av at det er en skyleveranse hvor tjenester for flere kunder produseres.

- 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.

  Svar: Standardkontrakter/rutiner skal utarbeides og tilstrebes innført for alle leverandører der hvor leveransens art og avtaleform gir rom for dette.

- 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.

  Svar: Det arbeides aktivt med sikkerhetslogging og analyse. Omfang utvides hele tiden, og vi er således enig i fokuset på dette området. Men vi er samtidig relativt godt fornøyd med det nivået vi har kommet oss opp på gjennom et sterkere operativt miljø i egen organisasjon.

Konklusjon
Basert på de utførte handlingene, innhentede bevis og organisasjonsdirektørens svar, er vi ikke blitt oppmerksomme på noe som gir oss grunn til å tro at Trondheim kommune ikke i det alt vesentlige har tilfredsstillende kontroll med tilganger til IT-systemene.

Denne uttalelsen er utelukkende utarbeidet for å gi kontrollutvalget et bedre grunnlag for å ivareta sitt påse ansvar med økonomiforvaltningen og til Trondheim kommunes informasjon, og er ikke nødvendigvis egnet til andre formål.

Med hilsen

Per Olav Nilsen
revisjonsdirektør

Børge Sundli
revisor/CISA

Elektronisk dokumentert godkjenning uten underskrift

Vedlegg: Brev til organisasjonsdirektøren av 150323
Svar fra organisasjonsdirektøren av 140423
Signert uttalelse fra ledelsen av 130423

Kopimottaker: Trude Kristin Kjeldstad, Organisasjonsdirektøren
Hilde Haugskott, Kontrollutvalgets sekretariat
Bjørn Jonny Villa, IT-tjenesten