Forvaltningsrevisjon IKT-sikkerhet i IKT Fjellregionen IKS - FARTT

Behandles i utvalg	**Møtedato**	**Saknr**
Kontrollutvalget i Tynset kommune	04.12.2023	41/23

Saksbehandler Ragnhild Aashaug
Arkivkode FE-217, TI-&58
Arkivsaknr 23/105 - 17

Forslag til vedtak
Forvaltningsrevisjonsrapporten IT-sikkerhet av 06.11.23 tas til orientering.

Tynset kommune følger revisors anbefalinger og kommunestyret ber eierrepresentanten for Fjellregionen IKT i samarbeid med kommunedirektøren om å sørge for at selskapet:

1. Iverksetter et arbeid med identifisering av informasjonsverdier, vurdering av trusler og sårbarheter som grunnlag for spesifikke sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganiseringen. Dette arbeidet kan munne ut i en overordnet plan for IKT og IKT-sikkerhet.
2. Avklare og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.
3. Vurdere å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.
4. Vurdere behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.
5. Utarbeide en plan for hendelseshåndtering og gjenoppretting.

Eierrepresentanten og kommunedirektøren rapporterer til kontrollutvalget om iverksatte tiltak innen 01.10.24.

Vedlegg
Forvaltningsrevisjon - IKT-sikkerhet FARTT

Saksopplysninger
Kontrollutvalget skal påse at forvaltningsrevisjon gjennomføres, jf. lov om kommuner og fylkeskommuner (kommuneloven) § 23-2 punkt c). Forvaltningsrevisjon innebærer å gjøre systematiske vurderinger av økonomi, produktivitet, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak og forutsetninger.
Rapport for forvaltningsrevisjon for IKT-sikkerhet i IKT Fjellregionen IKS er ferdigstilt og klar til behandling. Rapporten er bestilt av Tynset kommune og gjennomført som et samarbeidsprosjekt med Tolga, Alvdal og Rendalen kommuner

Tidligere behandlinger
Kontrollutvalget i Tynset tok initiativ til en forvaltningsrevisjon i FARTT ut fra at prosjektet var prioritert i kontrollutvalgets plan for forvaltningsrevisjon. I et felles møte for kontrollutvalgene i Nord-Østerdal den 14.november 2022, var samordning av kontroll i interkommunale samarbeid et tema. På bakgrunn av diskusjonen tok Tynset initiativ til en felles forvaltningsrevisjon for IKT.

- Sak 07/23 Invitasjon til deltagelse i forvaltningsrevisjon IKT-sikkerhet og personvern

Det ble sendt ut et forslag til prosjektskisse og hvordan kostnadene kunne fordeles. Alvdal, Rendalen og Tolga kommuner sluttet seg til prosjektet med forutsetning om finansiering fra kommunestyret.

- Sak 15/23 Prosjektplan for forvaltningsrevisjon av IT-sikkerhet og personvern

Arbeidet ble igangsatt i henhold til plan, og endelig rapport er levert den 6.11.2023. Rapporten ble noe forsinket siden det ble behov for avklaring av hvilken informasjon som kunne være offentlig med tanke på sikkerhetsrisiko. Etter en omarbeiding av rapporten er all informasjon offentlig.
Rapport for forvaltningsrevisjonen har vært på høring hos både kommunedirektørene i kommunene og daglig leder i FARTT. Etter høring har faktafeil i rapporten blitt korrigert. Høringssvarene fremgår av del 9 i rapporten, og et er verdt å merke seg at arbeidet med IKT-sikkerhet fra selskapet og i kommunene griper inn i hverandre.

Arbeidet med rapporten
Den viktigste målsettingen med prosjektet har vært å gi eierkommunene en ekstern vurdering av IKT-sikkerheten hos IKT Fjellregionen IKS (heretter kalt FARTT), samt å komme frem til mulige forbedringsområder som kan gi selskapet.

Forvaltningsrevisjonen har vurdert personvern i relasjon til god informasjonssikkerhet, blant annet ved vurdering av etablerte sikkerhetstiltak, tilgangsstyring og segregering av data. BDO har ikke gjennomført en analyse av FARTT sitt arbeid opp mot personvernlovgivningen utover dette. Revisjonen har i hovedsak omfattet felles infrastruktur som driftes av IKT Fjellregionen IKS på vegne av kommunene. Revisjonen har ikke omfattet infrastruktur driftet av andre eksterne parter eller av eierkommunene selv.

Revisjonskriterier gir vurderingsgrunnlaget for hva revisjonen skal vurdere opp mot. Denne revisjonen er i hovedsak basert på Norsk Sikkerhetsmyndighet (NSMs) grunnprinsipper for IKT-sikkerhet 2.0. Dette er et sett med prinsipper for hvordan IKT-systemer bør sikres for å beskytte verdier og leveranser.
Rapporten gir en utdyping av hvilke revisjonskriterier det er vurdert mot.

Metodene som er brukt for å svare ut problemstillingene er intervjuer, dokumentgjennomganger, penetrasjonstest og selvstendige analyser.
Vurderingskriteriene om hvordan undersøkte forhold avviker fra revisjonskriteriene er kategorisert i : *svært stor grad, stor grad, noen grad eller om* undersøkte forhold *møter i stor grad r*evisjonskriteriene.

Revisors problemstillinger med konklusjoner
Det er utarbeidet 5 problemstillinger, og revisor har konkludert for hver av de.

1. Styrer selskapet informasjonssikkerheten på en tilfredsstillende måte?
   Undersøkte forholdene avviker i noen grad fra revisjonskriteriene. Det er et forbedringspotensial knyttet til definering av roller og ansvar knyttet til informasjonssikkerhetsarbeidet, og oppdatering av styrende dokumenter.

2. Blir sikkerhetsrisikoer identifisert og håndtert?
   Undersøkte forhold avviker i stor grad fra revisjonskriteriene. Selskapet har kartlagt enheter og programvare som er i bruk, men innrullerte klienter i et forvaltningssystem først i 2023. Selskapet har kontroll på identiteter og tilganger på ansatte i kommunene, men det er et forbedringspotensial knyttet til gjestebrukere samt å begrense bruken av høyt privilegerte brukerkontoer. Kvaliteten på gjennomførte risiko- og sårbarhetsvurderinger vurderes å være svak.

3. Blir informasjon og informasjonssystemer beskyttet iht. beste praksis?
   De undersøkte forhold avviker i stor grad fra revisjonskriteriene. Det er avdekket flere betydelige svakheter i IKT-arkitektur og konfigurering. Selskapet gjør heller ingen sikkerhetsrevisjoner av underleverandører eller test av gjenoppretting og disaster

recovery. Rutinene knyttet til sikkerhetskopiering av virksomhetsdata for kommunene synes tilstrekkelig ivaretatt.

4. Hvordan oppdages avvik og mulige trusler mot virksomheten?
   De undersøkte forhold avviker i noen grad fra revisjonskriteriene. Det er etablert rutiner for sikkerhetsovervåkning og sårbarhetsscanning, men disse omfatter ikke oppfølging av varsler utenfor normal arbeidstid. Videre vurderer revisjonen at FARTT ikke har spesifikk kompetanse for å vurdere og håndtere cyberhendelser på en forsvarlig måte. Det er ikke tidligere gjennomført inntrengingstester.

5. Blir hendelser håndtert på en tilfredsstillende måte?
   De undersøkte forhold avviker i noen grad fra revisjonskriteriene. Selskapet har nylig revidert beredskapsplanverket, men handlingsplaner for utvalgte scenarioer virker ikke å være ferdigstilt. Selskapet gjennomfører evalueringer etter øvelser og hendelser, men har ikke rutiner for å gjennomføre tekniske øvelser. Dette gjør selskapet sårbart i håndteringen av nye og ukjente hendelser, ref. erfaringer fra hendelsen som inntraff høsten 2022

Revisjonens anbefalinger

1. Tydeliggjøre, beskrive og plassere det overordnede ansvaret for informasjonssikkerhet i FARTT.
2. Innføre standard herdeprofiler basert på beste praksis for PCer, servere og mobiltelefoner og innføre sikkerhetskonfigureringer i Microsoft 365 og Azure AD i henhold til beste praksis.
3. Etablere rutiner for sikkerhetsrevisjoner basert på kritikalitet og risiko.
4. Tilknytte seg en leverandør med spesifikk kompetanse innen cybersikkerhet som kan bistå med vurdering og håndtering av varsler og/eller ved cyberhendelser.

Vurdering og konklusjon

Revisjonen vurderer at FARTT har hatt et økende fokus på IT-sikkerhet, men at det gjenstår vesentlige forbedringer for å kunne stadfeste at FARTT har et tilfredsstillende IKT-sikkerhetsnivå. Gjennomgående for revisjonen er at FARTT har innført forbedringer det siste året, men at det fremdeles er en del avvik sett opp mot NSMs grunnprinsipper for IKT-sikkerhet og anerkjent beste praksis. Disse avvikene innebærer at FARTT og eierkommunene er sårbare for cyberangrep, og at det ved en større hendelse kan ta lengre tid enn nødvendig å oppdage angrepet, begrense og håndtere skadeomfanget, og gjenopprette systemene.

Revisjonens vurderinger er baseres på disse hovedfunnene:

- Manglende definering av roller og ansvar knyttet til informasjonssikkerhetsarbeidet.
- Det er avdekket flere betydelige svakheter i IKT-arkitekturen og konfigureringen til FARTT.
- FARTT gjør ingen sikkerhetsrevisjoner av underleverandører.
- FARTT har ikke etablert rutiner for å gjennomføre tekniske øvelser. Dette gjør selskapet sårbart i håndteringen av nye og ukjente hendelser.

Sekretariatet er av den oppfatning at BDO AS har avgitt en ryddig og tydelig rapport i tråd med vedtatt prosjektbeskrivelse.
I kommunedirektørens høring kommer det frem at det er en stor grad av samhandling mellom selskapet og kommunes drift for IKT-sikkerheten. Derfor foreslås det at kommunedirektør og eierrepresentant i fellesskap rapporterer om gjennomførte tiltak.
Det anbefales at kontrollutvalget slutter seg til rapporten og innstiller på revisors anbefalinger.