Oppfølging av forvaltningsrevisjon for IKT sikkerhet

Behandles i utvalg	**Møtedato**	**Saknr**
Kontrollutvalget i Tynset kommune	28.10.2024	32/24

Saksbehandler Ragnhild Aashaug
Arkivkode FE-217, TI-&58
Arkivsaknr 23/105 - 25

Forslag til vedtak
Kontrollutvalget tar rapporten om tiltak for forvaltningsrevisjon IKT sikkerhet til orientering. Kommunestyrets vedtak som gjelder forvaltningsrevisjon av IKT-sikkerhet i IKT Fjellregionen IKS anses som oppfulgt.

Vedlegg
Rapport tiltak Forvaltningsrevisjon IKT sikkerhet i FARTT

Saksopplysninger
Kontrollutvalgene i Tynset, Rendalen, Alvdal og Tolga har i fellesskap gjennomført en forvaltningsrevisjon av IKT-sikkerhet i selskapet IKT Fjellregionen. Samarbeidet mellom kommunene omtales som FARTT.

Dette vedtaket ble vedtatt av Tynset kommunestyre den 23.januar 2024 i sak 6/24:
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
I tillegg vedtok kommunestyret i Tolga et ekstrapunkt :

1. *Får tilgang på økt kompetanse på cyber-sikkerhet.*

For å følge opp anbefalingene, så utpekte kommunedirektørforum i FARTT-kommunene i januar 2024 en intern arbeidsgruppe. Arbeidet er sluttført, og det er utarbeidet en rapport. Til rapporten følger også vedlegg med detaljerte beskrivelser. Siden kontrollutvalget ikke pleier å gå inn i detaljene av hvordan anbefalingene følges opp, så ser ikke sekretariatet behovet for at vedleggene følger rapporten. Det er også gjort utfra en vurdering om at en publisering av fremgangsmåter kan utgjøre en ytterligere sikkerhetsrisiko.
Daglig leder i IKT Fjellregionen, Sverre Jenssen, vil presentere rapporten i møtet.
Representantskapet i IKT Fjellregionen er informert om arbeidet, og har gitt sin tilslutning til arbeidet med oppfølgingen.

Rapporten og arbeidet med anbefalingene
Rapporten viser hvordan det er arbeidet med å forsterke den generelle sikkerheten og oppfølgingen av de enkelte anbefalingene. Rapporten viser også hvordan utviklingen av IKT-sikkerhet på ulike områder skjer i samarbeid med kommunene (FARTT).

FARTT og eierkommunene bruker Compilo som styringssystem for informasjonssikkerhet. Compilo er et elektronisk verktøy hvor dokumenter samles i et elektronisk bibliotek.
Det er tatt utgangspunkt i personvernforordningen (GDPR) som grunnlag for tilstrekkelig informasjonssikkerhet, og kjøpt inn en GDPR-pakke fra Compilo til å forsterke sikkerheten. Kommunene og FARTT har utarbeidet GDPR prosessbeskrivelser som inngår i et årshjul for informasjonssikkerhet, som både FARTT og kommunene arbeider etter..

En gjennomgang av de enkelte anbefalingene

1. Overordnet plan for IKT og IKT-sikkerhet
   Det er igangsatt et arbeid med å identifisere informasjonsverdier, vurdere trusler og sårbarheter som grunnlag for spesifikke sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisering. Dette arbeidet har munnet ut i en overordnet plan for IKT og sikkerhet som omtales innledningsvis og gjennomgående i rapporten.
   a. Utarbeidelse av sikkerhetsmål for behandling av personopplysninger med formål, omfang og ansvarsavklaring (kapittel 5).
   b. Sikkerhetsstrategi for informasjonssikkerhet med formål, omfang, ansvarsavklaring og rutine for evaluering (kapittel 6).
   c. Mål for informasjonssikkerheten er at FARTT sine verdier skal ivaretas (kapittel 7).
   d. Identifisering av informasjonsverdier er utarbeidet etter hovedprinsippene konfidensialitet, integritet og tilgjengelighet (kapittel 8).
      Det er også gjort en klassifisering etter områder/sektor (kapittel 9).
   e. Risikostyring og risikovurdering av informasjonssikkerheten i FARTT
      Det er utarbeidet et system for risikovurdering ut fra kommunal informasjonssikkerhet sin modell (kapittel 14 og 15).

2. Organisering og ansvarsforhold i IKT sikkerhetsarbeidet
   Organiseringen og dokumenteringen av informasjonssikkerhetsarbeidet er utarbeidet og det er tildelt roller med definert ansvar. Det er også utarbeidet databehandleravtaler med leverandørene, utnevnt personvernombud og opprettet et sikkerhetsutvalg med definert ansvarsområde (kapittel 4).

3. Rutinen for tilgangsstyring er gjennomgått og det er innført et IAM-system som sikrer at brukere blir opprettet, endret og fjernet på en trygg og sikker måte. Det er også utarbeidet en rutine for utstyrshåndtering (kapittel 11).

4. Avvik og håndtering av avvik
   For dokumentasjon av IKT-hendelser som grunnlag for læring og evaluering så viser IKT Fjellregionen til Datatilsynets nettside om veileder for håndtering av avvik når det gjelder personvern. Det er også utarbeidet en mal for avvikshåndtering (kapittel 12).

5. Hendelseshåndtering og gjenoppretting
   Det samlede beredskapsplanverket for FARTT ligger i Compilo. Arbeidet med prosedyrer og rutiner for ulike hendelser har stort omfang, og arbeidet pågår fortsatt (kapittel 18).

6. Cybersikkerhet, kunnskap og kompetanse (oppfølgingspunkt fra Tolga).
   Det arbeides med å videreutvikle kompetansen hos ansatte i tillegg til at de kjøpes verktøy og tjenester fra ulike leverandører. Kompetanse på cybersikkerhet beskrives som mangelfullt på nasjonalt nivå (kapittel 19 og 20).

Vurdering
IKT Fjellregionen har sammen med en arbeidsgruppe fra eierkommunene utarbeidet en omfattende rapport for oppfølgingen som viser at arbeidet er tatt på største alvor. Hensikten med en forvaltningsrevisjon er å bidra til læring og forbedring, og det virker i aller høyeste grad som at det er oppnådd. Rapporten tar for seg sikkerhetsoppfølgingen utover de anbefalte oppfølgingspunktene, og det er positivt at IKT Fjellregionen setter dette arbeidet inn i en større sammenheng. Det bidrar også til å utvikle en større bevissthet om risikofaktorer for dette arbeidet både i selskapet og i kommunene.

I rapporten kommer det frem at IKT sikkerhet, informasjonssikkerhet og personvern er et kontinuerlig arbeid som må gjøres sammen med kommunene.
Kommunenes ansvar for å bygge en god sikkerhetskultur hos sine ansatte kommer igjen flere steder. Kontrollutvalget kan vurdere en egen oppfølging mot Tynset kommune for dette punktet på et senere tidspunkt. Det var i bestillingen av denne forvaltningsrevisjonen lagt opp til at kommunene kunne gjennomføre en egen forvaltningsrevisjon i den enkelte kommune for samhandlingen med IKT Fjellregionen og IKT-sikkerheten i den enkelte kommune.

I vedtaket bes kommunedirketør og eierrepresentanten om å rapportere til kontrollutvalget. Representantskapet i IKT Fjellregionen er kjent med utpekingen av arbeidsgruppa, og det arbeidet som er gjøres. Det ansees derfor ikke som nødvendig at eierrepresentanten skal møte.

Konklusjon
Oppfølgingen av forvaltningsrevisjonen av IKT-sikkerhet er vedlagt i en rapport. Arbeidet viser at det er gjennomført en oppfølging av alle anbefalingene som er satt inn i et helhetlig system.

Sekretariatet anbefaler at kontrollutvalget anser anbefalingene som oppfulgt. Kontrollutvalget kan på et senere tidspunkt vurdere en oppfølging mot kommunen og arbeidet som gjøres med å bygge en god sikkerhetskultur blant kommunens ansatte.