Rapport fra forvaltningsrevisjon om IKT sikkerhet

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Rennebu kommune	02.06.2023	19/23

Saksbehandler Ragnhild Aashaug
Arkivkode FE-217, TI-&58
Arkivsaknr 23/224 - 2

Forslag til vedtak:
Forvaltningsrevisjonsrapporten IT-Sikkerhet av 25.05.23 tas til etterretning.

Rennebu kommune følger revisors anbefalinger og kommunestyret ber kommunedirektøren sørge for å:

- Iverksette 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.
- Avklare og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.
- Vurdere å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.
- Vurdere behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.
- Utarbeide en plan for hendelseshåndtering og gjenoppretting.

Kommunedirektøren rapporterer til kontrollutvalget om iverksatte tiltak innen 01.12.23.

Vedlegg
IT- sikkerhet rapport- endelig

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.

I kontrollutvalgsmøtet 03.05.2022, sak 24/22, orienterte IKT-rådgiver og personal- og stabssjef om hvordan den digitale sikkerheten ivaretas i Rennebu kommune. I denne saken vedtok kontrollutvalget følgende:
Ut fra en generell risiko- og vesentlighetsvurdering mener kontrollutvalget at det bør gjennomføres en forvaltningsrevisjon innenfor IT-sikkerhet. Også Nasjonal Sikkerhets-myndighet har kommet med klare råd til virksomheter om å forebygge og avverge cyberangrep. Forvaltningsrevisjon innen IT-sikkerhet står ikke i plan for forvaltnings-revisjon. På den bakgrunn ber kontrollutvalget om at en forvaltningsrevisjon på dette området blir prioritert og gjennomføres utenom planen.
Kontrollutvalget oversender saken til kommunestyret med følgende forslag til vedtak: Kommunestyret ber kontrollutvalget om å gjennomføre en forvaltningsrevisjon innenfor IT-sikkerhet utenom gjeldende plan for forvaltningsrevisjon.

Kommunestyret behandlet saken 16.06.2022, sak 22/2022, og ba om at det det gjennomføres en forvaltningsrevisjon innenfor IT-sikkerhet.
Dette vedtaket er bakgrunn for kontrollutvalgets bestilling 21.09.2022.
Prosjektplanen ble behandlet av kontrollutvalget den 09.11.22.

Problemstillinger:

Følgende to problemstillinger besvares i rapporten:

1. *Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?*

Følgende revisjonskriterier er utledet for denne problemstillingen:

- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen skal ha sikkerhetsmål og sikkerhetsstrategi.
- Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjons-sikkerhet framgår.
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
- Kommunen må ha rutiner med tilhørende praksis for tildeling og fjerning av tilganger og jevnlig kontrollere identiteter og tilganger.
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.
- Kommunen bør vurdere og dokumentere IKT-risiko ved anskaffelser av datasystemer.
- Kommunen bør evaluere og lære av hendelser.

2. *Har kommunen tilfredsstillende tekniske og organisatoriske tiltak for å ivareta informasjonssikkerhet?*

Følgende revisjonskriterier er utledet for denne problemstillingen:

- Identifisere og kartlegge
    - Kommunen må ha en oversikt over enheter i IKT-systemet.
    - Kommunen bør ha en oversikt over programvare.

- Beskytte og opprettholde
    - Kommunen bør etablere og dokumentere en sikker IKT-arkitektur.
    - Kommunen bør ha sentral styring med sikkerhetsoppdateringer.
    - Kommunen må ha en plan for sikkerhetskopiering og ta sikkerhetskopier.

- Oppdage
    - Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen.
    - Kommunen bør gjennomføre inntrengningstester.

- Håndtere og gjenopprette
    - Kommunen bør ha en plan for hendelseshåndtering (ansvar, tiltak, kommunikasjon, gjenopprettingsplan og loggføring).
    - Kommunen må ha en plan for gjenoppretting.

Metode:
Metodene som er brukt for å svare ut problemstillingene er intervju med sentrale personer i kommunene som har en rolle i forhold til informasjonssikkerhet og dokumentgjennomgang. Etter revisjonens mening gir dette et tilstrekkelig innsyn i kommunens system og rutiner knyttet til informasjonssikkerhet. Sekretariatet har ingen forutsetninger for å gjøre ytterligere vurderinger.

Det er gjennomført intervjuer med kommunedirektør, personal- og stabssjef, IKT-rådgiver og innkjøpskoordinator for å få frem detaljer om informasjonssikkerhet. Det er gjort både

separate og felles intervjuer med ledelsen (som omfatter kommunedirektør og personal- og stabssjef). I tillegg er det gått gjennom dokumentasjon som er oversendt fra kommunen og systemet for risikovurderinger og avviksmeldinger.

Kommunedirektørens uttalelse:
En foreløpig rapport ble sendt til kommunedirektøren for uttalelse, 30.03.2023. Revisjon Midt-Norge SA mottok svar 27.04.2023. Uttalelsen er vedlagt rapporten (vedlegg 2).

Sammen med uttalelsen fra kommunedirektøren fikk revisor tilbake foreløpig rapport med korrigeringer i henhold til beskrivelsen i uttalelsen fra kommunedirektøren. Der går det fram at direkte feil er merket med gjennomstreking av tekst, mens tilføyelser er skrevet i rødt. Revisor har gått gjennom forslagene til korrigeringer. I korrigeringene kommer det delvis ny informasjon, som revisor har bedt om mer dokumentasjon på og revisor stilte i tillegg noen oppfølgingsspørsmål i epost 04.05.2023. Revisor mottok dokumentasjon og svar 10.05.2023. Svarene fra 10.05.2023 er gjengitt i vedlegg 3.

Korrigeringer i uttalelsen fra kommunedirektøren som er påpekninger av feil er rettet.

Revisors hovedkonklusjon:
På bakgrunn av funnene konkluderer revisor med at:

- Rennebu kommune har sentrale mangler i styringssystemet for informasjonssikkerhet. Det mangler spesifikke sikkerhetsmål, sikkerhetsstrategi og en tydelig sikkerhetsorganisasjon.

- Rennebu kommune har flere tekniske og organisatoriske tiltak for å ivareta informasjons-sikkerheten, men mangler kritiske planer for hendelser og gjenoppretting.

Revisjonens anbefalinger:
Revisor har følgende anbefalinger til kommunen:
- Iverksette 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.
- Avklare og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.
- Vurdere å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.
- Vurdere behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.
- Utarbeide en planer for hendelseshåndtering og gjenoppretting.

Vurdering:
Sekretariatet er av den oppfatning at Revisjon Midt-Norge SA har avgitt en rapport i tråd med vedtatt prosjektbeskrivelse.
Sekretariatet anbefaler at kontrollutvalget slutter seg til rapporten og videresender den til kommunestyret for endelig behandling.