Behandling av forvaltningsrevisjonsrapport - Beredskapsplan og IT-sikkerhet

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Vefsn kommune	08.04.2025	09/25

Saksbehandler Kent Røstad
Arkivkode FE-217, TI-&58
Arkivsaknr 24/167 - 9

Forslag til vedtak
Kontrollutvalget tar rapporten til orientering og legger den fram for kommunestyret med følgende innstilling:

1. Kommunestyret tar rapport fra forvaltningsrevisjon om beredskap og informasjonssikkerhet i Vefsn kommune til orientering.
2. Kommunestyret ber kommunedirektøren sørge for at:
    a. informasjonssikkerhet inngår i kommunens overordna ROS-analyser og beredskapsplan.
    b. det vurderes hvilke informasjonsverdier kommunen har, og sørge for at styringssystemet for informasjonssikkerhet ivaretar alle informasjonsverdier.
    c. informasjonssikkerheten systematisk overvåkes og analyseres.
    d. det gjennomføres inntrengningstester.
    e. protokollen for personopplysninger inneholder alle system og programvare som kommunen har, og gjøre de obligatoriske og anbefalte vurderingene.
    f. opplæring i informasjonssikkerhet settes i system.
3. Kommunestyret ber kommunedirektøren gi en skriftlig tilbakemelding til kontrollutvalget innen den 14. november 2025 om hvordan punkt 2 i vedtaket er fulgt opp

Vedlegg
Forvaltningsrevisjonsrapport - Beredskap og informasjonssikkerhet

Saksopplysninger
Kontrollutvalget bestilte den 25. april 2024 (sak 14/24) en forvaltningsrevisjon om beredskapsplan og IT-sikkerhet i Vefsn kommune. Prosjektplan ble lagt fram i kontrollutvalgets møte 13. september 2024 i sak 27/24. I prosjektplanen argumenterte revisor for at det var fornuftig at prosjektet omfatter *informasjonssikkerhet*, da det omfatter mer enn IT.

Revisor utarbeidet følgende problemstillinger for forvaltningsrevisjonen:

- Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?
- Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

Prosjektplan med forvaltningsrevisors forslag til vinkling og problemstillinger ble vedtatt i sak 27/24.

Metode
Intervju
Revisor har gjennomført fem individuelle intervju nøkkelpersoner innen informasjonssikkerhet i Vefsn kommune. Alle som er intervjuet, er del av en gruppe for Kompetansegruppe for informasjonssikkerhet og personvern (KIP) i kommunen.

Dokumentgjennomgang
Revisor har gjennomført dokumentgjennomgang. Viktige dokumenter som revisor har fått tilsendt er:

- Overordna prosedyre for informasjonssikkerhet
- Personvernprosedyre
- ROS-analyser
- Beredskapsplaner
- Avviksrapporter
- Andre, relevante rutiner og prosedyrer

Gjennomgang disse dokumentene har vært benyttet til å vurdere om kommunen har tilfredsstillende styrende dokumenter, rutiner og prosedyrer for informasjonssikkerhet.

Systemgjennomgang
I forbindelse med besøket i Vefsn kommune fikk revisor en gjennomgang av om, og hvordan dokumentasjon er lagt til rette i kvalitetssystemet Compilo. Revisor har ikke hatt gjennomgang av andre systemer.

Revisors funn
Revisor har undersøkt om Vefsn kommune har nødvendig informasjonssikkerhet. Det har revisor gjort ved å belyse to problemstillinger:

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

- Revisor konkluderer med at kommunen langt på vei har etablert et slikt styringssystem.
- Kommunen har et styringsdokument for informasjonssikkerhet med sikkerhetsmål og beskrivelse av sikkerhetsansvar og -organisering. Informasjonssikkerhet er inkludert i kommunens system for internkontroll.
- Etter revisors vurdering er ansvar og organisering klart definert i prosedyren for informasjonssikkerhet. KIP-gruppen har en viktig rolle i arbeidet med informasjonssikkerhet. Gruppen er relativt ny, og har ikke et formalisert mandat. Etter revisors vurdering er medlemmenes deltakelse i møter gruppa variabel. Arbeidet i gruppen er lite formalisert.
- Kommunen har en for avgrenset forståelse av informasjonssikkerhet, slik det kommer fram i prosedyren for informasjonssikkerhet. Den tar ikke høyde for alle informasjonsverdier som kommunen har.
- Det er en svakhet at overordna ROS og beredskapsplan ikke berører trusler som gjelder informasjonssikkerhet. Det kommer heller ikke fram i den overordna beredskapsplanen. Trusler mot informasjonssikkerhet er blant de største risikoene kommuner har stått overfor de siste tiårene.
- Kommunen har en beredskapsplan for IT-sikkerhet. Den virker, etter revisors vurdering generell, og ikke spesielt rettet inn mot beredskap for IT-sikkerhet i virksomhetene i Vefsn kommune.
- Etter revisors vurdering har kommunen etablert et system (regneark) for å føre protokoll over hvilke personopplysninger de behandler. Systemet synliggjør hva som skal være obligatoriske vurderinger og andre anbefalte vurderinger, men oversikten over systemer er mangelfull, og
  det mangler obligatoriske opplysninger for flere system.
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet. Selv om det informeres om dokumenter som ansattes må lese, er det en risiko for at det ikke følges opp i praksis, siden det ikke er signaturløsning. Unntaket er opplæring for sykepleiere og vernepleiere, som skal signere opplæring i pasientjournal. Innen arkivområdet skjer opplæringen en-til-en.

- Det kan stilles spørsmål ved den generelle opplæringen i organisasjonen i informasjonssikkerhet

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

- Revisor konkluderer med at kommunen langt på vei har slike tiltak.
- Revisor vurderer at kommunen har en praksis hvor det er bestiller av systemet (systemansvarlige) som er ansvarlig for å følge opp systemet; at det blir utarbeidet en databehandleravtale og risiko- og sårbarhetsanalyse.
- Revisor vurderer at kommunen gjennom å ha dokumentert fysiske strukturer for kommunens lokasjoner, bidrar til å dokumentere IKT-arkitekturen. Samtidig er det mange sikkerhetsfunksjoner og ulike IKT-produkter som må fungere godt og sikkert sammen. Kommunen har ikke fått på plass et godkjent konfigurasjonskart i henhold til sin egen prosedyre som revisor vurderer som en svakhet.
- IKT-avdelingen sørger for faste tidspunkt for sikkerhetsoppdateringer på kommunens PCer. For kommunens egne systemer, er revisor usikker på hvilken rutine som gjelder for sikkerhetsoppdateringer. Systemansvarlig er ansvarlig for oppdateringer knyttet til andre system.
- Kommunen har en praksis for sikkerhetskopiering og tar sikkerhetskopier.
- Det er en svakhet at kommunen ikke har tilfredsstillende planer for håndtering og gjenoppretting av hendelser.
- Revisor vurderer at kommunen ikke har tilfredsstillende system for å overvåke sikkerheten og analysere data fra overvåkningen.
- Kommunen gjennomfører heller ikke inntrengningstester da det er opplyst at kommunen ikke har hatt tid eller ressurser til å gjennomføre dette.
- Vefsn kommunen er medlem av HelseCert som gjennomfører ekstern overvåkning, men revisor er ikke kjent med hvordan loggene fra HelseCert følges opp i kommunen. Videre vurderer revisor at kommunen ikke har etablert et system for å overvåke sikkerheten og analyse av data. Kommunen har ikke etablert overvåkning av sine egne systemer.
- Kommunen er i gang med å utarbeide en beredskapsplan innenfor IKT. Revisor vurderer at planen framstår som et utkast og er ikke tilpasset Vefsn kommune. Ved en hendelse må kommunen klare seg selv, for de har ingen eksterne avtaler med for eksempel en SOC- tjeneste. Revisor vurderer at kommunen i liten grad har planer som dekker kommunens behov dersom det skjer en krise på informasjonssikkerhet slik at datasystemet er mer eller mindre utilgjengelig over flere dager.
- Utkastet til beredskapsplanen er ikke oppdatert med en vurdering av kommunens systemer med tanke på gjenoppretting til en normaltilstand etter en hendelse. Kommunen svarer selv at de vil prioritere system innenfor helse og omsorg.
- Revisor konkluderer videre med at oversikten over programvare som er oversendt, er mangelfull. Det er ikke alle programmer som kommer fram i oversikten, og det er heller ikke alle obligatoriske og anbefalte opplysninger som er fylt ut.

Revisor anbefaler

Revisor anbefaler at kommunedirektøren sørger for at:

- informasjonssikkerhet inngår i kommunens overordna ROS-analyser og beredskapsplan
- vurdere hvilke informasjonsverdier kommunen har, og sørge for at styringssystemet for informasjonssikkerhet ivaretar alle informasjonsverdier
- informasjonssikkerheten systematisk overvåkes og analyseres
- det gjennomføres inntrengningstester
- protokollen for personopplysninger inneholder alle system og programvare som kommunen har, og gjøre de obligatoriske og anbefalte vurderingene
- opplæring i informasjonssikkerhet settes i system

Kommunedirektøren har fått oversendt ferdig rapport til uttalelse. Kommunedirektøren har informert sekretariatet om at det ikke anses nødvendig å gi ytterligere tilbakemelding til rapporten før behandling i kontrollutvalget.

Forvaltningsrevisor Anna Ølnes vil møte i kontrollutvalgets møte 8. april 2025 og presentere rapporten.

Vurdering
Sekretariat mener at revisor har svart ut problemstillingene som var satt for forvaltningsrevisjonen, og at rapporten gir nyttig informasjon om beredskap og IT-sikkerhet i Vefsn kommune.