RM Revisjon Midt-Norge

Beredskap og informasjonssikkerhet

Vefsn kommune

Forvaltningsrevisjon

2025

FR1301

FORORD

Denne forvaltningsrevisjonen er gjennomført på oppdrag fra kontrollutvalget i Vefsn kommune. Forvaltningsrevisjonen er gjennomført etter NKRFs (Kontroll og revisjon i kommunene) standard, Standard for forvaltningsrevisjon (RSK 001)

Vi vil takke alle som har bidratt med informasjon i prosjektet.

Alle rapporter fra Revisjon Midt-Norge SA publiseres på www.revisjonmidtnorge.no.

Trondheim, 14.03.2025

Anna Ølnes — Oppdragsansvarlig forvaltningsrevisor

Hanne Marit Ulseth Bjerkan — Prosjektmedarbeider

SAMMENDRAG

Kontrollutvalget i Vefsn kommune bestilte den 25.04.2024, sak 14/24, en forvaltningsrevisjon om beredskap og IT-sikkerhet. Denne rapporten oppsummerer forvaltningsrevisjon om Vefsn kommune har nødvendig informasjonssikkerhet. Det har vi gjort ved å belyse to problemstillinger:

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

Vi har gått mer i dybden på saks- og arkivsystem og helsejournaler.

I kapittel 1.3 beskriver vi begrepet «informasjonssikkerhet». KS har utarbeidet en veileder om informasjonssikkerhet og personvern som er et tillegg til veilederen om internkontroll. Her forklares informasjonssikkerhet som vern av alle typer informasjon, for eksempel opplysninger om kommunens innbyggere, ansatte, vannverk, økonomi eller kommunens servicetilbud. Ulik type informasjon vil ha forskjellig beskyttelsesbehov. Beskyttelsesbehovet kan deles opp i tre, ifølge veilederen; konfidensialitet, integritet, og tilgjengelighet. Konfidensialitet innebærer at informasjonen ikke blir kjent for uvedkommende. Integritet betyr at informasjon ikke blir endret utilsiktet eller av uvedkommende. Tilgjengelighet er at informasjon er tilgjengelig ved behov. Denne veilederen, i tillegg til lover og forskrifter om informasjonssikkerhet og personvern, har vært kilder for utledning av revisjonskriterier (vedlegg 1). Veiledningsmateriale fra Datatilsynet og Nasjonal sikkerhetsmyndighet har også vært kilder for revisjonskriterier.

For å få tilfredsstillende datagrunnlag for vurderinger og konklusjoner har vi gjennomført individuelle intervju med nøkkelpersoner innenfor informasjonssikkerhet i Vefsn kommune. Videre har vi etterspurt og gjennomgått det vi har fått tilsendt av styrende dokumenter, prosedyrer og rutinebeskrivelser som kommunen har utarbeidet. Vi har dessuten fått en gjennomgang av hvordan styrende dokument og rutiner er gjort tilgjengelig i kvalitetssystemet Compilo. Vi har også fått oversikter over avviksmeldinger som gjelder informasjonssikkerhet, og oppfølging av disse. Dette er nærmere beskrevet i kapittel 1.4.

Et utkast til rapport har vært sendt til uttalelse hos kommunedirektøren. Kommunedirektøren har ikke avgitt uttalelse.

På problemstillingen **om kommunen har etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket**, konkluderer revisor med at kommunen langt på veg har etablert et slikt styringssystem (kapittel 4). Kommunen har et styringsdokument for informasjonssikkerhet med sikkerhetsmål og beskrivelse av sikkerhetsansvar og -organisering. Revisor vil også trekke fram at informasjonssikkerhet er inkludert i kommunens system for internkontroll. Revisor ser likevel en del svakheter i systemene for informasjonssikkerhet. Revisor mener at 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.

Videre konkluderer revisor med at det er en svakhet at overordna risiko- og sårbarhetsanalyse (ROS) og beredskapsplan ikke berører trusler som gjelder informasjonssikkerhet. Trusler mot informasjonssikkerhet er blant de største risikoene kommuner har stått overfor de siste tiårene. Revisor mener videre, at det kan stilles spørsmål ved den generelle opplæringen i organisasjonen i informasjonssikkerhet.

Revisjonskriterier, datagrunnlag og vurderinger som bygger opp om denne konklusjonen er utdypet i kapittel 2.

På problemstillingen **om kommunen har tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet**, konkluderer revisor med at kommunen langt på vei har slike tiltak (kapittel 4). Revisor mener 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. 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.

Revisjonskriterier, datagrunnlag og vurderinger som bygger opp om denne konklusjonen er utdypet i kapittel 3.

På bakgrunn av vurderinger og konklusjon anbefaler revisor kommunedirektøren å sørge 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

INNHOLDSFORTEGNELSE

Figurer

1 INNLEDNING

1.1 Bestilling

Kontrollutvalget i Vefsn kommune bestilte den 25.04.2024, sak 14/24, en forvaltningsrevisjon om beredskap og IT-sikkerhet. I protokollen gikk det fram noen tema som kontrollutvalget ønsket å få belyst. Disse temaene kan oppsummeres som beredskapsplaner for IT-området, opplæring og øvelser knyttet til kommunens IT-beredskap, løsninger for opprettholdelse og gjenoppretting av virksomheten ved bortfall saks- og arkivsystem, samt helsejournaler. I forbindelse med prosjektplanleggingen sammenfattet revisor disse temaene i to problemstillinger (nedenfor) og foreslo noen begrepsmessige endringer: I bestillingen ble begrepet IT-sikkerhet og IT-beredskap brukt, mens revisor foreslo for kontrollutvalget å bruke begrepet informasjonssikkerhet og lignende begrep. Kontrollutvalget sluttet seg til det da prosjektplanen ble lagt fram og vedtatt den 13.9.2024 i sak 27/24.

I kapitlene 1.2 og 1.3 beskrives problemstillingene og temaet informasjonssikkerhet nærmere.

1.2 Problemstillinger

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

Vi har gått mer i dybden på saks- og arkivsystem og helsejournaler.

1.3 Informasjonssikkerhet

KS har utarbeidet en veileder, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet[1]. Den er et tillegg til Kommunedirektørens internkontroll – Orden i eget hus[2]. I veilederen forklares informasjonssikkerhet som vern av alle typer informasjon, for eksempel opplysninger om kommunens innbyggere, ansatte, vannverk, økonomi eller

[1] KS og KPMG.

[2] KS, «Orden i eget hus - kommunedirektørens internkontroll», 2020, https://www.ks.no/globalassets/fagomrader/lokaldemokrati/internkontroll/Kommunedirektorens-internkontroll-veileder-F41-web.pdf.

kommunens servicetilbud. Ulik type informasjon vil ha forskjellig beskyttelsesbehov. Beskyttelsesbehovet kan deles opp i tre, ifølge veilederen; konfidensialitet, integritet, og tilgjengelighet. Konfidensialitet innebærer at informasjonen ikke blir kjent for uvedkommende. Integritet betyr at informasjon ikke blir endret utilsiktet eller av uvedkommende. Tilgjengelighet er at informasjon er tilgjengelig ved behov.

I KS´ veileder forklares sammenhengen mellom personvern og informasjonssikkerhet. Personopplysninger er en type informasjon som skal beskyttes. Personvernforordningen (GDPR) har dreid fokuset til informasjonssikkerhet noe over mot sikkerhet for personopplysninger. Informasjonssikkerhet er imidlertid mer enn personvern, på samme måte som personvern er mer enn informasjonssikkerhet. Personvern og informasjonssikkerhet overlapper når det gjelder beskyttelsen av personopplysninger.

KS ´veileder forklarer også begrepet informasjonsverdi. All informasjonen kommunen eier, og behandler har en verdi. Verdien varierer ut fra typen informasjon og hvilken type virksomhet informasjonen tilhører. Informasjon i denne sammenhengen er alt fra kunnskap, personopplysninger, forretningshemmeligheter, beregningsmodeller, informasjon om hvordan saksbehandlingen skal gjennomføres, IKT-systemer hvor informasjon blir behandlet, teknisk infrastruktur mv. Det å kjenne sine verdier er viktig i informasjonssikkerhetssammenheng, ettersom det avgjør hvordan den skal beskyttes. Beskyttelsesgraden vurderes ut ifra hvor viktig informasjonen er, og hvordan behovet for konfidensialitet, tilgjengelighet og integritet skal bli ivaretatt.

I veilederen forklares personopplysninger og personvern. Personopplysninger er enhver opplysning om en identifiserbar eller identifisert person. Personvernet skal bidra til å verne om personopplysninger og er knyttet til enkeltindividets rett til privatliv, selvbestemmelse og selvutfoldelse. Viktige elementer i personvernet er at den enkelte skal ha kontroll over, og i størst mulig grad kunne bestemme over egne personopplysninger. Dette omtales ofte som personopplysningsvern.

Nasjonal sikkerhetsmyndighet (NSM) skriver på sine nettsider[3] at sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å beskytte verdiene mot tilsiktede, uønskede handlinger. Risikovurdering, risikohåndtering, sikkerhetskontroll og hendelseshåndtering inngår i dette arbeidet. Gjennom systematiske kontroller og god styring på aktivitetene kan

[3] https://nsm.no/fagomrader/sikkerhetsstyring/hva-er-sikkerhetsstyring/

virksomheten avdekke sårbarheter og håndtere uønskede hendelser knyttet til verdiene som virksomheten forvalter.

Målet med sikkerhetsstyring, ifølge NSM, er å styre sikkerhetsarbeidet for å oppnå og opprettholde et forsvarlig sikkerhetsnivå, basert på den risiko virksomheten er eksponert for.

Sikkerhetsstyring bør ses i sammenheng med sikkerhetskultur. NSM skriver at sikkerhetskultur handler om atferd knyttet til sikkerhet, eksempelvis informasjon eller objekter[4].

NSM har utarbeidet en veileder i sikkerhetsstyring, Veileder i sikkerhetsstyring[5]. Denne er en av flere kilder som ligger til grunn for utledning av revisjonskriteriene opp mot. Lovverk knyttet til informasjonssikkerhet som er sentralt i revisjonen, er Lov om nasjonal sikkerhet[6] og Lov om behandling av personopplysninger[7]. Disse, og annet regelverk og veiledere er utdypet i vedlegg 1, om utledning av kriterier.

1.4 Metode

Forvaltningsrevisjonen er gjennomført i henhold til NKRFs standard for forvaltningsrevisjon, RSK 001. Revisor har vurdert egen uavhengighet overfor Vefsn kommune, jf. kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon kapittel 3.

For å belyse de to problemstillingene og de tilhørende underpunktene, har vi kombinert flere metoder for å få et samla datagrunnlag. Vi innledet prosessen med et oppstartsmøte med kommunedirektøren og ledere og nøkkelpersonell i organisasjonen med ansvar og oppgaver i tilknytning til temaet. Her la vi fram problemstillinger og overordna revisjonskriterier, i tillegg til at vi fikk oppnevnt kontaktperson, som har bistått oss med dokumentasjon og koordinering av intervjuavtaler. Nedenfor beskriver vi mer inngående de ulike metodene og om de hver for seg og til sammen har fungert etter intensjonen.

[4] https://nsm.no/fagomrader/sikkerhetsstyring/sikkerhetskultur/

[5] Nasjonal sikkerhetsmyndighet (NSM), «Veileder i sikkerhetsstyring», 2020, https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-sikkerhetsstyring/om-denne-veilederen/.

[6] Justis- og beredskapsdepartementet, «Lov om nasjonal sikkerhet (Sikkerhetsloven)», 2018.

[7] Justis- og beredskapsdepartementet, «Lov om behandling av personopplysninger (personopplysningsloven)», Pub. L. No. LOV-2018-06-15-38 (2018), https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=lov%20om%20behandling%20av%20personopplysninger.

Intervju

Vi har gjennomført i alt fem individuelle intervju, basert på en delvis strukturert spørsmålsliste (intervjuguide). De vi har intervjuet er:

- Fagansvarlig for HMS-system og leder av KIP-gruppen (gruppe for informasjonssikkerhet) og vår kontaktperson i revisjonsprosessen. Heretter omtales denne funksjonen som «sikkehetsansvarlig».
- IKT-ansvarlig i kommunen
- Personvernombudet (kommuneadvokat) i kommunen
- Systemansvarlig helse- og omsorgstjenester
- Leder for fellestjenester (arkiv)

Alle som er intervjuet, er del av en gruppe for Kompetansegruppe for informasjonssikkerhet og personvern (KIP) i kommunen. Alle intervjuene skjedde ved fysisk tilstedeværelse. Det ble skrevet referat fra hvert av intervjuene, og alle har godkjent aktuelle referat.

Det er sendt oppfølgingsspørsmål på epost til flere av de vi har intervjuet. IKT-leder har fått en liste med spørsmål som han i hovedsak har svart ut.

Intervjuinformasjonen dekker utdypende informasjon om organisering, system og styringsdokument for informasjonssikkerhet. Gjennom intervjuene har vi også fått svar på ledere og nøkkelpersoners forståelse av og erfaringer med kommunens informasjonssikkerhet.

Dokumentgjennomgang

Vi har etterspurt og fått tilsendt dokumentasjon fra kontaktpersonen vår og fra de vi har intervjuet. Dette er dokumentasjon av dokument, prosedyrer og rutiner som skal være styrende og støttende for arbeidet med informasjonssikkerhet. Viktige dokumenter som vi 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 vi en gjennomgang av om, og hvordan dokumentasjon er lagt til rette i kvalitetssystemet Compilo. Vi har ikke hatt gjennomgang av andre systemer.

Vurdering av metode

Vi vurderer at kombinasjonen av metoder og data sikrer et tilfredsstillende grunnlag for vurderinger og konklusjoner på problemstillingene. Vi har ikke intervjuet andre enn de som er medlemmer i KIP-gruppen. Det betyr at vi ikke har informasjon om ansattes erfaringer med og praktisering av informasjonssikkerhet. Vi har ikke testet systemene og rutinene i kommunen, så vi har ikke informasjon om styrke og svakheter utenom det som har kommet fram i metodene som er beskrevet ovenfor. Vi sendte en liste med spørsmål til IKT-leder etter intervjuet, som han svarte ut. Et oppfølgingsintervju kunne ha lagt til rette for utdypning, men vi vurderte at spørsmålslisten var mest effektiv, totalt sett, for oss og IKT-leder.

1.5 Uttalelse om rapport

En foreløpig rapport ble sendt til kommunedirektøren for uttalelse den 27.2.2025. Kommunedirektøren, ved sikkerhetsansvarlig har svart at de ikke vil gi uttalelse. Det er derfor ikke noen uttalelse vedlagt rapporten.

2 STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET

I dette kapittelet vurderer revisor om kommunen har etablert et system for informasjonssikkerhet.

2.1 Problemstilling

Det er utarbeidet følgende problemstilling for temaet:

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

2.2 Revisjonskriterier

- Kommunen skal ha et overordna, oppdatert styringssystem for informasjonssikkerhet som angir sikkerhetsmål og sikkerhetsstrategi for kommunens informasjonsverdier
- Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår.
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må gjennomføre risikovurderinger og dokumentere vurderinger av personvernkonsekvenser.
- Kommunen skal føre protokoll over hvilke personopplysninger de behandler.
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.

Revisor viser til vedlegg 1, for kilder for og utledning av kriterier.

2.3 Funn

I dette kapitlet legger vi fram informasjon fra dokumenter, system og intervjuer.

2.3.1 System for informasjonssikkerhet

Kommunen må ha et overordnet system for informasjonssikkerhet, som angir sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisasjon for kommunens informasjonsverdier.

Innledningsvis spurte vi de vi intervjuet om hva de *forstår med informasjonssikkerhet:*

- At informasjonen som kommunen lagrer eller sender ikke bryter med GDPR, og at denne informasjonen blir beskyttet. Informasjonssikkerhet betyr videre at kommunen har de riktige systemer, som ROS-analyser og databehandleravtaler.
- Den er todelt: Alle retningslinjer og prosedyrer for ansatte for skjerming av informasjon. I tillegg; sikre robuste systemer, tilpasset kommunens virksomhet.
- Sørge for at GDPR og forvaltningslovens personvernbestemmelser etterfølges.
- Sikre kommunens datasystemer mot trusler, sammenbrudd, rutinebrudd (f.eks. utskrifter, personlister osv.).
- For min rolle handler det om å ivareta personopplysninger på en sikker måte.
- Jeg legger i informasjonssikkerhet, å beskytte verdier som skal skjermes. I det daglige å låse skjerm når man går fra arbeidsplassen og passe på passordene sine. Det innebærer også riktige tilganger til riktig behov.

Beskrivelsene ovenfor varierer, men flere peker i retning beskyttelse av personvernopplysninger.

Revisjonen har etterspurt styrende dokumenter for informasjonssikkerhet. Vi har fått oversendt flere dokumenter, blant annet et dokument med navnet Informasjonssikkerhet i Vefsn kommune (heretter kalt prosedyre for informasjonssikkerhet). Det framgår av dokumentet at prosedyren ble administrativt vedtatt av kommunedirektøren i 2006. Etter det har prosedyren blitt revidert i 2013, 2017, 2019, 2020 (to ganger) og siste gang 12. oktober 2024. I dokumentet framgår følgende overordna mål med informasjonssikkerhet:

> Bruk av elektroniske hjelpemidler ved behandling av personopplysninger gjør det mulig å utnytte kommunens ressurser mer optimalt. Samtidig vil en slik bruk introdusere nye trusler overfor de opplysninger som behandles. Kommunens overordnede mål for elektronisk behandling av personopplysninger er derfor en effektiv, men tilstrekkelig sikker, saksbehandling.

I kapittel 2, om strategiske sikkerhetsmål framgår det følgende:

> Ved manuelle og elektroniske behandlinger av personopplysninger skal opplysningene sikres tilstrekkelig:
>
> - **konfidensialitet**, slik at opplysningene ikke blir kjent for uvedkommende
> - **tilgjengelighet**, slik at alle medarbeiderne med tjenestelig behov kan utføre pålagte oppgaver, og brukerne av kommunens tjenester gis tilfredsstillende informasjon
> - **integritet**, slik at opplysningene ikke utilsiktet endres

> Kommunen skal ha et bevisst forhold til de ekstra risikoer som gjelder ved elektronisk behandling av personopplysninger. Sikkerhetstiltak skal gi god margin i forhold til sikkerhetsbehovet.

Prosedyren har et eget kapittel om sikkerhetsstrategi for informasjonssikkerhet. Her framgår følgende deler:

- Ansvars- og myndighetsforhold
- Organisering av informasjonssystemet
- Systemteknisk sikkerhet og fysisk sikring
- Personellsikkerhet
- Partnere og leverandører

Vi spurte de vi intervjuet om kommunens styringssystem for informasjonssikkerhet. Ansvarlig for informasjonssikkerhet viste til prosedyren for informasjonssikkerhet og de andre dokumentene som revisor fikk oversendt før intervjuene:

- Personvernprosedyre
- Helhetlig ROS-analyse 2018
- Redigert godkjent beredskapsplan 2023
- Personalmapper; hva skal hvor

Vi kommer tilbake til disse dokumentene utover i kapittelet.

De andre vi intervjuet viste også til prosedyren, Informasjonssikkerhet i Vefsn kommune.

IKT-leder fortalte at kommunen ikke har tatt i bruk NIS 2[8]. Han var opptatt av at kommunens lokale prosedyrer må være egnet for at kommunens ledelse og ansatte kan ta eierskap til dokumentene, og da kan de ikke bare implementere NIS 2 som den er. Det er et veldig omfattende sett av prosedyrer. Kommunens prosedyrer inneholder, etter IKT-leders mening, alt som skal med, men i en litt kortfattet versjon. Han fortalte at styringssystemet for informasjonssikkerhet ble laget lenge før den nye personvernforordningen ble vedtatt i 2018. Styringssystemet ble laget etter mal fra Datatilsynet. Det styringssystemet kommunen jobber for å få implementert nå, baserer seg på ISO 27000 og anbefalinger fra NSM.

[8] Europaparlaments- og rådsdirektiv (EU) 2022/2555 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer (Vedlegg/protokoll XI i EØS-avtalen.)

2.3.2 Sikkerhetsledelse og sikkerhetsorganisering

Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår.

I prosedyren for informasjonssikkerhet er ansvar, myndighetsforhold og organisering av informasjonssikkerhet beskrevet i to kapitler: I kapittelet om sikkerhetsstrategi for informasjonssikkerheten (kapittel 3.1) og i kapittel 4 om ansvars- og myndighetsforhold for informasjonssikkerheten.

Funksjon	**Ansvar**
Kommunedirektøren	Har det overordnede ansvaret for informasjonssikkerheten i kommunen.
Enhetsledere	Skal påse at tilfredsstillende sikkerhet oppnås ved behandling av personopplysninger innen den enkeltes myndighetsområde/enhet.
IKT-leder	Har ansvaret for driftstekniske oppgaver i tilknytning til informasjonssystemene og har det overordnet operativt ansvar for drift av informasjonssystemene.
Fagleder HMS/kvalitet	Det overordnet operativt ansvar for informasjonssikkerheten og er heretter benevnt som sikkerhetsansvarlig.
Systemansvarlig	Det skal utpekes systemansvarlig for hvert av kommunens informasjonssystemer.
Kompetansegruppe for informasjonssikkerhet og Personvern (KIP)	Instruksjonsmyndighet over enhetsledere og systemansvarlige for så vidt gjelder disse forhold. KIP rapporterer direkte til kommunedirektøren.

Figur 1. Ansvar for informasjonssikkerhet. Kilde: Prosedyre for informasjonssikkerhet. Vefsn kommune.

I kapittel om ansvars- og myndighetsforhold er ansvaret til de ulike funksjonene konkretisert for kommunedirektøren og strategisk ledergruppe, KIP, sikkerhetsansvarlig, enhetsledere, IKT-leder, systemansvarlige, kommunearkivar, den enkelte ansatte og personvernombudet.

Sikkerhetsansvarlig er leder av KIP-gruppa. Han sa at KIP-gruppa svarer rett til kommunedirektør og det er kommunedirektør som tar avgjørelser. KIP-gruppa har delegerte oppgaver, men ikke myndighet og ansvar. Sikkerhetsansvarlig sa at gruppa ble etablert for et års tid siden, og samtidig fikk han rollen som sikkerhetsansvarlig. Han var ikke kjent med om noen har hatt denne rollen tidligere. Gruppen har ikke noe skriftlig mandat utover det som er beskrevet i prosedyre for informasjonssikkerhet.

I begynnelsen var det faste, månedlige møter, ifølge sikkerhetssjefen. Etter et par måneder har møtehyppigheten avtatt, og det holdes møter ved behov. Behovene kan meldes fra alle i gruppa, men det er sikkerhetsansvarlig som har ansvaret for å kalle inn til møter og skrive referat. Gruppa har avholdt et møte i forbindelse med denne revisjonen.

De øvrige som vi intervjuet, hadde i varierende grad deltatt i møter. Fagleder for e-helse har ikke hatt funksjonen så lenge, og har ikke deltatt i så mange møter. Arkivleder har deltatt noe lenger, og hun sa at gruppen blant annet har sett på behandlingsprotokoller. Personvernombudet deltar også i gruppen, og ga uttrykk for at kommuneledelsen har relativt god struktur på dette. Han trakk fram systemkontroll, som eksempel på temaer som har vært tatt opp i gruppen.

2.3.3 Informasjonssikkerhet i kommunens internkontroll

Informasjonssikkerhet skal inngå i kommunens internkontrollsystem. I prosedyre for informasjonssikkerhet er det et avsnitt om internkontroll, og målet med internkontroll:

> Målet med internkontroll er å etablere og holde vedlike iverksatte tiltak for å oppfylle kravene lov og forskrift stiller i forbindelse med behandling av personopplysninger, og evt. gjøre endringer eller iverksette nye tiltak ved behov.

Videre står det at det er enhetsleder som er ansvarlig for gjennomføring av internkontroll i sin enhet. Internkontroll skal skje ved hjelp av kommunens kvalitetssikringssystem og dokumenteres i henhold til dette.

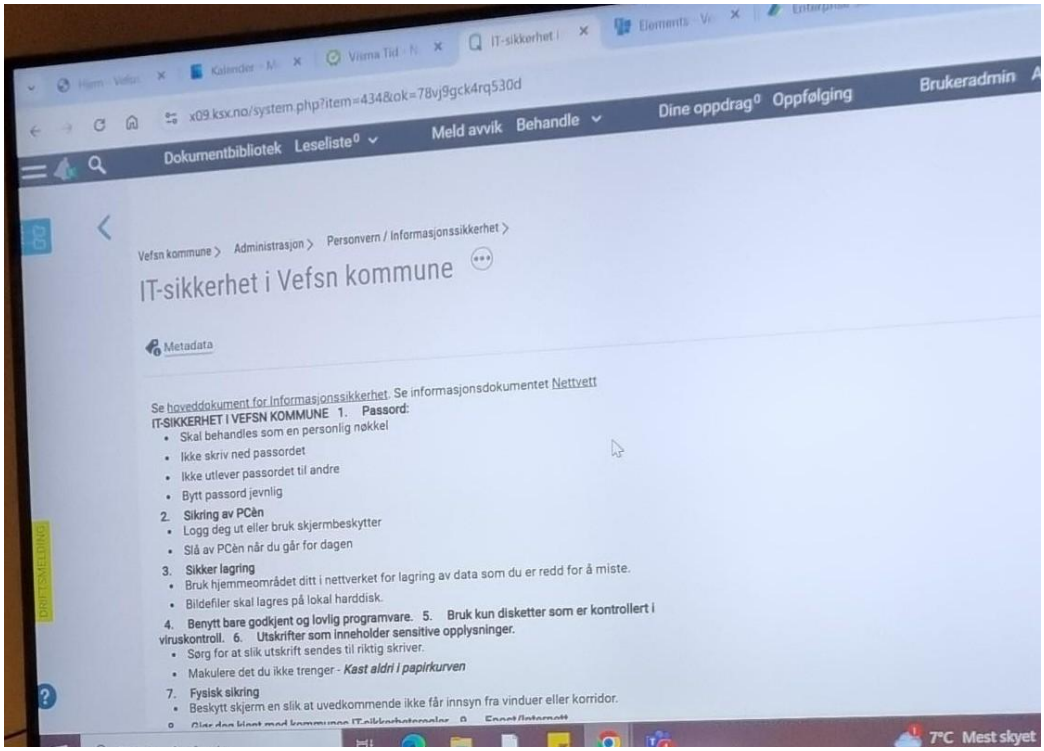
Vefsn kommune bruker Compilo som kvalitetssystem. Sikkerhetsleder gikk gjennom systemet med revisor, med fokus på hvilke styrende dokumenter som er tilgjengelig i Compilo, og avvikshåndtering for informasjonssikkerhet.

Prosedyre for informasjonssikkerhet og prosedyre for personvernopplysninger er tilgjengelig i dokumentbiblioteket i Compilo. Gjennomgangen viste flere andre dokument som også var tilgjengelige i Compilo, som Beredskapsplan for IT-sikkerhet. Revisor sjekket ikke nærmere om alle, relevante dokument var tilgjengelig der.

Fagleder for e-helse fortalte at det til en viss grad er utarbeidet rutiner innen hennes område, men viste til rutine for håndtering av elektroniske meldinger, CosDoc. Det er en rutinehåndbok for CosDoc som skal revideres. Fagleder har overtatt ansvaret for CosDoc.

Fagleder for e-helse hadde ikke vært delaktig i utarbeiding eller revidering av den generelle rutinen for informasjonssikkerhet i kommunen. For hennes område er det Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren hun fokuserer på, en bransjenorm som baserer seg på lovverket rundt dette. Det er en veileder som de bruker til å sikre at vi følger de lover og regler som gjelder innenfor dette området.

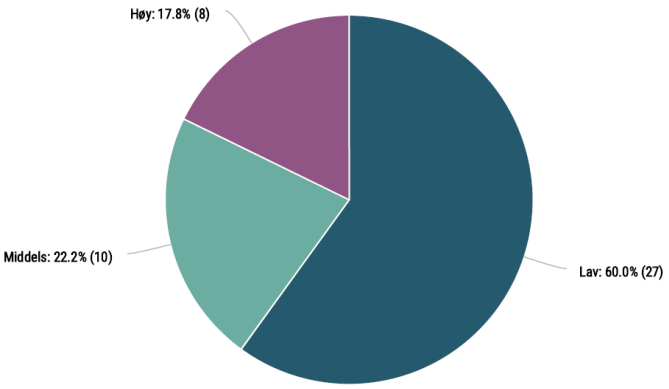
Nedenfor viser vi eksempel på hvordan styrende dokument er gjort tilgjengelig i Compilo:



Figur 2. Bilde av dokument i dokumentbiblioteket i Compilo. Revisjon Midt-Norge

Vi fikk også en gjennomgang av avvikssystemet (i Compilo). Sikkerhetssjefen er systemadministrator og har tilgang til avviksmodulen. Personvernombudet får også melding når det meldes avvik knyttet til informasjonssikkerhet. Det er nærmeste leder som mottar og håndterer meldte avvik. Dette går også fram av prosedyren for informasjonssikkerhet. Det er en egen kategori for personvernopplysninger/informasjonssikkerhet. Det ble meldt 45 avvik på informasjonssikkerhet i 2024, går det fram av Compilo.

Figuren nedenfor viser andel (antall) avvik innen tre alvorlighetsgrader. Flertallet av avvikene, 60 prosent, har lav alvorlighetsgrad, mens de øvrige fordeler seg på 22 prosent for middels og 18 prosent for høy alvorlighetsgrad.



Figur 3. Alvorlighetsgrad for meldte avvik for personvernopplysninger/informasjonssikkerhet GDPR. 2024

Vi har fått avviksrapporter fra januar 2025 og tilbake til 2020. Rapporterte avvik for personopplysninger og informasjonssikkerhet har økt i disse årene.

I 2023 var det rapportert 31 avvik innenfor denne kategorien, der andelen middels alvorlighetsgrad var høyest av de tre alvorlighetsgradene (39 prosent).

Av de 45 meldte avvikene i 2024, gjaldt 23 personopplysninger på avveie og de øvrige 9 gjaldt tilgang til informasjon/system.

Fagleder for e-helse fortalte at det er skilt ut for å melde avvik på personvern. Avviket går til leder på avdelingen og til personvernombudet. Tekniske avvik blir synliggjort, og det er fagleders ansvar, som systemansvarlig, å følge opp dette. Hun får beskjed om de tekniske avvikene fra leder som har mottatt avviket.

Arkivleder hadde ikke opplevd avviksmeldinger for systemene som hun er ansvarlig for. Kontrollen de gjennomfører før postlisten publiseres, har oppdaget eventuelle avvik og avvik har da blitt korrigert. Kontrollene fungerer, og det blir ikke meldt avvik, ifølge arkivleder.

Sikkerhetssjefen sa at typiske avvik som er meldt, er ulåste skap og kontordører og gjenglemt papir på skriver.

Sikkerhetssjefen har jobbet mye med å få ansatte til å melde avvik. Det er tema på personalmøter og hver avdeling har et kvalitetsutvalg (verneombud og tillitsvalgt) hvor avvik også tas opp.

2.3.4 Risikovurderinger av informasjonssikkerhet

Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.

Revisor har fått tilsendt et utvalg av risiko- og sårbarhetsanalyser (ROS). Den ene er helhetlig, overordna ROS-analyse for Vefsn kommune, datert 2018. En gjennomgang av dokumentet viser at det ikke inneholder risikovurderinger knyttet til informasjonssikkerhet, noe sikkerhetssjefen også bekrefter.

I prosedyre for informasjonssikkerhet er det et eget kapittel om risikovurderinger. Her defineres risiko som «potensialet for tap av konfidensialitet, integritet og tilgjengelighet i tilknytning til personopplysninger: liv/helse, økonomi og/eller anseelse/integritet for enkeltmennesker». Det framgår av prosedyren at det er enhetsleder som er ansvarlig for gjennomføring av risikovurderinger. Risikovurderinger skal gjennomføres i følgende tilfeller:

- før oppstart av ny behandling
- i forbindelse med endringer i konfigurasjonen
- i forbindelse med organisatoriske endringer av betydning for informasjonssikkerheten
- i forbindelse med fysiske endringer på steder hvor personopplysninger lagres /oppbevares
- når det er avdekket sikkerhetsbrudd

Videre, framgår det at det skal være en årlig gjennomgang til ledelsen. Revisor har ikke etterspurt skriftlig dokumentasjon på innholdet i denne gjennomgangen.

I avsnittet om risikovurdering framgår det også beskrivelse av risikovurdering ved personopplysninger. Dette kommer vi tilbake til.

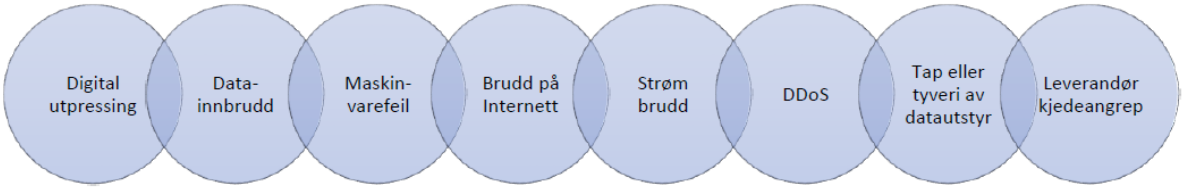
Risikovurderinger skal sammenholdes med kriterier for akseptabel risiko. Tiltak skal settes inn der det er sprik mellom disse.

Vefsn kommunes overordna beredskapsplan ble sist revidert 7. februar 2024. Det går ikke fram beskrivelser av beredskap for informasjonssikkerhet i beredskapsplanen.

Sikkerhetssjefen sa at det er gjennomført risikovurderinger for de ulike systemene i kommunen. Disse risikovurderingene ligger lagret sammen med databehandleravtalene. IKT-leder har laget et system i Excel som viser denne oversikten og lenke til saksnummer i Elements for å finne avtale og risikoanalyse.

Vi har fått tilsendt et dokument, Beredskapsplan IT. Dokumentet er udatert, men etter referansene til ISO-standarder å dømme, er den utarbeidet etter 2022. I toppteksten står det at dokumentet er en del av kommunens styringssystem for informasjonssikkerhet. Dokumentet har ikke referanser til beredskap for virksomhetene i Vefsn kommune.

I en figur, som vist nedenfor, framgår IT-relaterte uønska hendelser (scenarier).



Figur 4. IT-relaterte, uønska hendelser (scenarier). Kilde: Beredskapsplan IT, Vefsn kommune

For hver hendelse beskrives hendelsen nærmere i en oversikt:

Digital utpressing	Beskrivelse
	Risikovurdering
	Sikkerhetstiltak
	Respons (som etablering av kriseledelse)

Figur 5. Eksempel på beskrivelse, risikovurdering, tiltak og respons for uønsket hendelse.

Et tredje dokument vi har fått tilsendt er Plan for kriseberedskap, sykehjemstjenesten, hjemmetjenesten og miljøterapitjenesten. Planen skal oppdateres årlig, og den versjonen vi har fått tilsendt ble oppdatert 5. januar 2024. Vi har gjennomgått planen. Beredskapsplanen inneholder noen elementer om risiko og beredskap som kan knyttes til informasjonssikkerhet. Det gjelder kapittel 10.4 Scenario 3: Skade på kritisk infrastruktur. Her er sikring av tilgang til journalsystem, bortfall av trygghetsalarm, papirversjoner av pasientjournal eksempler på tiltak.

Fagleder for e-helse fortalte at det fortløpende lages risikovurderinger for nye system, som CosDoc. Hun mente at ROS-analysene burde oppdateres.

Vi har også mottatt to dokumenter, ROS-GDPR Elements og ROS Databehandleravtale Jupiter. Elements er saks- og arkivsystemet til kommunen. Her framgår det risiko-, sannsynlighets- og konsekvensvurderinger for 13 hendelser fordelt på 3 risikoobjekt: Hendelser knyttet til autentisering, hendelser knyttet til dataangrep, og hendelser knyttet til rutinebrudd.

Jupiter er systemet som har vært brukt for å legge ut dokumenter til møter i kommunestyre, formannskap og andre utvalg. Risikovurdering for dette systemet inneholder risiko-, sannsynlighets- og konsekvensvurderinger for én hendelse: Sensitive opplysninger blir publisert. Avtalen med Jupiter er sagt opp, forteller arkivleder, og det er inngått avtale med ny leverandør. Vi har ikke sett ROS-analyse av dette systemet. Arkivleder sa at det ikke er gjort ROS-analyse av arkivplanen.

2.3.5 Vurdering av personvernkonsekvenser (DPIA)

Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.

IKT-leder fortalte at systemansvarlige gjør personkonsekvensvurderinger (DPIA) ved innføring av nye system. Han viste til personvernombudet, som har sagt at kommuner arbeider etter lovverk som ivaretar DPIA-bestemmelsene i utgangspunktet. Derfor er det ikke påkrevd at kommuner utarbeider personvernkonsekvensutredninger. Dette bekreftet personvernombudet i intervju.

Revisor har forhørt seg med fungerende juridisk direktør og seksjonssjef for offentlige tjenester i Datatilsynet om dette stemmer. Tilbakemeldingen var følgende:

> Offentlige myndigheter skal ha rettslig grunnlag i for eksempel lov eller forskrift når de behandler personopplysninger, for eksempel gjennom opplæringslov, barnevernlov, helselovgivningen osv. Dette krav til rettslig grunnlag og såkalt supplerende grunnlag følger av personvernforordningen artikkel 6. Kravet til å gjennomføre personvernkonsekvensvurderinger (DPIA) følger av artikkel 35 i personvernforordningen. Det er gjort unntak fra kravet om å gjennomføre slike vurderinger når en behandling er regulert i lov (eller forskrift) og at man i forbindelse med etableringen av dette rettslige grunnlaget har gjennomført vurderinger av personvernkonsekvenser. Likevel kommer artikkel 35 til anvendelse dersom man tar i bruk ny teknologi som kan ha høy risiko for enkeltpersoner. Det kan for eksempel være

plikt til å gjennomføre DPIA hvis man vil ta i bruk inngripende kunstig intelligens (KI). Kommunen må vurdere i hvert enkelt tilfelle om det må gjennomføres en DPIA.

Informasjonen fra personvernombud og kontaktperson i Datatilsynet viser at det er spesielle regler for kommuner.

2.3.6 Protokoll for behandling av personopplysninger

Kommunen skal føre protokoll over hvilke personopplysninger de behandler. En av pliktene er at alle virksomheter som behandler personopplysninger, skal føre protokoll over behandlingsaktivitetene de har ansvar for (artikkel 30 i personopplysningsloven). Protokollen skal inneholde formålet med behandlingen, hvilke kategorier personopplysninger kommunen behandler, tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Dersom det er aktuelt, skal eventuelle databehandlere stå oppført i protokollen.

IKT-leder har sendt et regneark, Protokoll behandlingsansvarlig Vefsn kommune. Oversikten viser 23 kolonner, som omfatter alt fra «system» til databehandleravtalens saksnummer i Elements. Protokolloversikten inneholder formål, kategori av registrerte, personopplysninger og kategori av mottakere. Videre inneholder den tidsfrist for sletting og generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak. IKT-leder fortalte at kommunen har mellom 70 – 80 system. Det er oppført 49 system i protokollen. For under 20 av systemene er det oppgitt formål med behandlingen (obligatorisk), og det mangler obligatoriske opplysninger for flertallet av systemene i skjemaet.

Ifølge arkivansvarlig har KIP-gruppa hatt behandlingsprotokoller oppe og sett på innholdet flere ganger.

2.3.7 Opplæring i informasjonssikkerhet

Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet. I informasjonssikkerhetsprosedyren går det fram at kommunens ansatte skal ha tilstrekkelig kompetanse og gis nødvendig opplæring, slik at sikkerheten opprettholdes.

Sikkerhetssjefen fortalte at nyansatte får beskjed om hvilke dokumenter de skal lese. Det er et ønske om å få til en leseliste i Compilo som de ansatte må følge opp og signere når de har fullført. Han sa videre at ansatte må signere taushetserklæring.

Vi har også fått oversendt et dokument, opplæringsbevis CosDoc. Sykepleiere og vernepleiere skal krysse ut for en rekke opplysninger som gjelder CosDoc generelt, hovedkort, arbeidsplan og pasientjournal og signere på skjemaet.

Arkivleder fortalte at to medarbeidere i hennes avdeling sørger for opplæring. Opplæringen skjer på PC-en til den nyansatte, i hovedsak en-til-en-opplæring. Det har også vært gjennomgang og opplæring i utvidet ledergruppe. I tillegg veiledes det på telefon ved behov.

Det er enhetsledere som skal påse at de ansatte har tilstrekkelig kunnskaper om bruk av informasjonssystemene og nødvendig kompetanse i informasjonssikkerheten, før det gis tilgang.

2.4 Revisors vurdering

I dette kapittelet vurderer revisor situasjonen som er beskrevet i kapittel 2.3 opp mot kriteriene.

2.4.1 System for informasjonssikkerhet

Kommunen skal ha et overordna styringssystem for informasjonssikkerhet som angir sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisasjon.

Kriteriet er delvis oppfylt

Etter revisors vurdering har Vefsn kommune et system for informasjonssikkerhet, gjennom prosedyre for informasjonssikkerhet. Den ivaretar innhold som overordna mål, sikkerhetsmål og organisering av informasjonssikkerhet. Etter revisors vurdering er forståelsen av informasjonssikkerhet og prosedyrer for dette for avgrenset til personopplysninger, sett opp mot myndigheters definisjon av informasjonssikkerhet og informasjonsverdier. Prosedyren ble sist revidert i oktober 2024, men etter revisors vurdering har det vært lite regelmessighet i revideringen av prosedyren. Kommunen har en beredskapsplan for IT-sikkerhet. Revisor kan ikke se at den er tilpasset utfordringer som gjelder Vefsn kommune.

2.4.2 Sikkerhetsledelse og sikkerhetsorganisering

Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår.

Kriteriet er delvis ivaretatt

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.

Sikkehetsledelse er, etter revisors vurdering en liten del av en stilling, og har blitt skjøvet til side på grunn av andre oppgaver, også ifølge sikkerhetssjefen.

2.4.3 Informasjonssikkerhet i kommunens internkontrollsystem

Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.

Kriteriet er oppfylt

Revisor vurderer at informasjonssikkerhet inngår i kommunens internkontrollsystem, ved at viktige styringsdokumenter for informasjonssikkerhet er tilgjengelig i Compilo. Det rapporteres avvik på personopplysninger og informasjonssikkerhet.

2.4.4 Risikovurderinger av informasjonssikkerhet

Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.

Kriteriet er mangelfullt oppfylt

Etter revisors vurdering er det en svakhet at informasjonssikkerhet og trusler mot denne ikke er berørt i kommunens overordna ROS-analyse. Det kommer heller ikke fram i den overordna beredskapsplanen.

I prosedyren for informasjonssikkerhet er det eget kapittel om risikovurderinger. Det foreligger også dokument for risikovurderinger for flere system, men etter revisors vurdering er det manglende oppfølgingen av i praksis.

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. Dette temaet berøres også i kapittel 3.3.2 og 3.3.6 revisors vurdering.

2.4.5 Vurdering av personvernkonsekvenser

Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.

Kriteriet er delvis oppfylt

Disse risikovurderingene er ivaretatt i mye av lovverket som kommunen forholder seg til, men ikke alt. Revisor ser en viss risiko for at kommunen tolker at de ikke trenger å gjøre risikovurderinger av DPIA i det hele tatt. Det kan medføre at risikovurderinger knyttet til personvernkonsekvenser ikke er utført og dokumentert der de skulle ha vært det.

2.4.6 Protokoll for behandling av personopplysninger

Kommunen skal føre protokoll over hvilke personopplysninger de behandler.

Kriteriet er mangelfullt oppfylt

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, som formål med behandling av personopplysninger, for flere system. Protokollen skal ha vært tema i flere KIP-møter. Etter revisors vurdering mangler flere system i regnearket, og det mangler obligatoriske vurderinger for flere av systemene.

2.4.7 Opplæring i informasjonssikkerhet

Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.

Kriteriet er mangelfullt oppfylt

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.

3 ORGANISTATORISKE OG TEKNISKE TILTAK

I dette kapittelet vurderer revisor om kommunen har tilfredsstillende organisatoriske og tekniske tiltak på bakgrunn av innsamlet datagrunnlag.

3.1 Problemstilling

Det er utarbeidet følgende problemstilling for temaet:

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

3.2 Identifisere og kartlegge

3.2.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen må ha en oversikt over enheter i IKT-systemet.
- Kommunen bør ha en oversikt over programvare.
- Kommunen må ha et system for styring av tilganger.

Utledningen av revisjonskriteriene finnes i vedlegg 1.

3.2.2 Oversikt over enheter

IKT-leder forteller at IKT-tjenesten i kommunen har oversikt over alle enhetene som kommunen har. Alle PCer som brukes til kommunale formål er kjøpt av kommunen. Kommunen bruker System Center Configuration Manager (SCCM, nå Microsoft System Center Configuration Manager) for å holde oversikt over kommunens PCer. For nettbrett brukes Intune[9], hvor kommunen har oversikt over antall og modell. IKT-leder forteller at tilganger fjernes for PCer som ikke har vært i kontakt med nettverket over en viss periode.

For kommunalt eide nettbrett og telefoner, forteller IKT-leder at det benyttes flåtestyring for disse. NSM definerer flåtestyring som et verktøy for å kunne administrere mobile enheter fra sentralt hold. Flåtestyring gjør det mulig å håndheve retningslinjer der det som et minimum er

[9] Intune er en skytjeneste som administrere klienter, hvilke data ulike bruker kan få tilgang til og hva de kan gjøre med dataene.

begrensninger på hvilke applikasjoner som kan installeres, og fjernsletting om enheter blir mistet eller stjålet, ifølge NSM.[10]

Kommunen har brannmur og servere i et låst rom på rådhuset hvor kun autoriserte personer har tilgang.

3.2.3 Oversikt over programvare

IKT-leder uttaler at det er ca. 70-80 system i kommunen. IKT-leder viser til at kommunen har et regneark med oversikt over kommunens system med opplysninger om blant annet systemansvarlige og databehandleravtaler. Regnearket er utarbeidet av IKT-leder ifølge sikkerhetsansvarlig.

Revisor har fått oversendt regnearket, og det er registrert 49 system. Systemansvarlig er utfylt for 12 av systemene.

3.2.4 Tilgangsstyring

I dokumentet «Informasjonssikkerhet i Vefsn kommune» er det et eget kapittel for personellsikkerhet. Kapitlet beskriver at ansatte kun gis tilgang til personopplysninger i informasjonssystemet i den grad det er nødvendig for å utføre pålagte oppgaver. Før tilgang gis, skal ansatte med tjenstlig behov ha tilstrekkelig kunnskap om bruk av informasjonssystemet og nødvendig kompetanse i informasjonssikkerhet. Alle ansatte skal videre informeres om den taushetsplikt og rutiner som gjelder.

Videre i dokumentet, beskrives ansvars- og myndighetsforhold for informasjonssikkerheten. Det framkommer at enhetsledere har ansvaret for å avgjøre hvilke ansatte som har tjenstlig behov for tilgang til hvilke personopplysninger og hvilke deler av informasjonssystemene. Videre skal enhetsledere melde fra om endringer av tjenstlig behov ved endring i arbeidsoppgaver eller ansatte som slutter.

Dokumentet «Personvern og informasjonssikkerhet – den ansattes plikter» inneholder også en del om tilgangsstyring, blant annet at det er kommuneledelsens ansvar å legge til rette for at den enkelte ansatte kun får tilgang til de opplysninger som vedkommende trenger for å utføre sine oppgaver. Tilgangsstyringen skal sørge for at det er begrenset hva den enkelte kan se av opplysninger, at den enkelte sin bruk av informasjonssystemet blir hendelsesregistrert (logget), og at hendelsesregisteret blir kontrollert for å avdekke eventuelle sikkerhetsbrudd.

[10] Kilde: Mobilapplikasjoner på tjenesteenheter, 2024, Temarapport, NSM.

Dokumentet presiserer med visning til helsepersonelloven at det er forbud mot såkalt snoking (urettmessig tilegnelse av taushetsbelagte opplysninger).

IKT-leder opplyser at Vefsn kommune benytter eADM[11], som automatiserer tilganger ved bruk av lønns- og personalsystemet. Ved nyansettelser sender leder personalmelding til HR-avdelingen og IKT-seksjonen mottar melding via deres servicedesk om hvilke tilganger den nyansatte skal ha. Sikkerhetsansvarlig forteller at det er hver enkelt leder som har ansvaret for å følge opp tilgangen til sine ansatte.

På spørsmål om rutiner for avslutning av tilganger, svarer IKT-leder at tilgangen via påloggingen til PC avsluttes når vedkommende slutter. Sikkerhetsansvarlig forteller at ved avslutning av tilganger, sender leder epost til IKT. IKT-seksjonen sender videre til systemadministratorer, men sikkerhetsansvarlig mener at kommunen er litt dårlig på å etterleve denne praksisen. Tilganger kan fortsatt henge igjen selv etter at folk har sluttet. Videre forteller sikkerhetsansvarlig at flere skybaserte system i kommunen er tilknyttet opp mot den kommunale eposten, og IKT-seksjonen sletter denne eposten når ansatte slutter.

Systemansvarlige har ansvar for tilganger til de ulike fagsystemene, ifølge IKT-leder. IKT-leder forteller at det er en målsetning om å ha singel-sign-on-pålogging (SSO) som tillater at brukere får tilgang til flere systemer eller applikasjoner med bare én pålogging.

Rutinehåndboken for elektronisk meldingsutveksling (tilknyttet helse) inneholder rutine for nytt helsepersonell i CosDoc. Rutinen gjelder for IT og ledere. Det er databehandlingsansvarlig/avdelingsleder som er ansvarlig for at tilgang administreres slik at tilgang til helse- og personopplysninger kun gis ved tjenstlig behov. Rutinen beskriver hvilke krav/aktiviteter som skal gjennomføres til en tidsfrist og hvem som er ansvarlig for dette. Systemansvarlig for CosDoc innenfor helse forteller at tilgang gis ut ifra kompetanse/stilling og avdeling til de ansatte. Sykepleier og hjelpepleier har ulike tilgangsbehov, og de ansatte har kun tilgang til sin respektive avdeling. Ansatte som jobber nattevakt, har en annen tilgang på grunn av at de betjener flere avdelinger.

Ved endring i arbeidssted eller avslutting av arbeidsforhold, omtaler rutinehåndboken at det settes en sluttdato for stillingen (evt. opprettes ny stilling for aktuelle avdeling) og ved avslutning av stillingen avautoriseres brukeren i CosDoc. Ansvarlig for dette er

[11] eADM effektiviserer tildelingen og tilbakekallingen av tilgangsrettigheter ved å automatisere disse prosessene for å sikre nøyaktig tildeling og en robust IKT-sikkerhet. Kilde: https://www.identum.no/products-eadm

avdelingsleder/systemansvarlig ifølge rutinen. Ved avslutning av arbeidsforhold, forteller systemansvarlig for CosDoc at avdelingsleder kan avslutte tilgangen. Det er avdelingsleder som kjenner til om den ansatte har et arbeidsforhold eller ikke, og som avgjør om det er behov for tilgang til pasientens journals. Hvis avdelingsleder ikke kan gjøre dette selv, sender de forespørsel til systemansvarlig som avslutter tilgangen. Systemansvarlig forteller at per januar 2025 er ikke avslutninger av tilganger like godt innarbeidet. Som systemansvarlig gjennomfører hun en til to ganger i året en kontroll, sammen med avdelingsleder, for å se om riktige personer har tilganger.

For Elements (sak- og arkivsystem) forteller systemadministrator at det er ledere i kommunen som bestiller tilgang til sine ansatte. Forespørsel om tilgang kommer via servicedesken eller via epost. Systemadministrator forteller at det ikke er noen skriftlige rutiner knyttet til tilgangsstyringen. På spørsmål om hvilke rutiner de har for avslutning av tilgang, forteller systemadministrator at leder skal melde inn i god tid før ansatte slutter. Arkiv tar en sjekk av status for saksbehandleren (vedkommende som slutter) og følger opp at uferdige/ubesvarte poster blir besvart/ferdigstilt eller flyttet til ny saksbehandler. Systemadministrator vil videre stenge tilgangen i Elements ut fra opplysningen som er gitt av leder. Tilganger både til produksjonsbase og historiske baser stenges og den ansatte fjernes fra tilgangs- og saksbehandlergrupper den har vært medlem av.

3.2.5 Revisors vurdering

Kommunen må ha en oversikt over enheter i IKT-systemet.

Revisor vurderer kriteriet som oppfylt.

Kommunen har oversikt over enheter i IKT-systemet.

Kommunen bør ha en oversikt over programvare.

Kriteriet er delvis oppfylt

Kommunen har laget seg et regneark over systemene i kommunen. Revisor vurderer at det er noe usikkert hvor oppdatert regnearket er knyttet til antall systemer og innhold. Revisor ser at ikke alle systemer i kommunen er registrert i regnearket, samt at ikke alle opplysninger er fylt ut for alle system. Revisor vurderer derfor at oversikten over programvare framstår noe mangelfull og ikke oppdatert. Det er viktig, ifølge NSM å ha oversikt over hvilken programvare som befinner seg i kommunen før en potensiell angriper gjør det.

Kommunen må ha et system for styring av tilganger.

Revisor vurderer kriteriet som delvis oppfylt.

Revisor finner at Vefsn kommune har knyttet tilgangsstyringen til lønns- og personalsystemet. Når det gjelder avslutning av tilganger er revisor mer usikker på om det styres gjennom HR-systemet. Informasjon tyder på at systemet ikke er helt fullstendig per i dag.

3.3 Beskytte og opprette

3.3.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.
- 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.

Utledningen av revisjonskriteriene finnes i vedlegg 1.

3.3.2 Anskaffelser

I dokumentet «Informasjonssikkerhet i Vefsn kommune», under ansvars- og myndighetsforhold er ansvaret for å avklare hvem som skal være systemansvarlig når nye system anskaffes lagt til IKT-leder. Videre har enhetslederne ansvaret for å se til at det ikke kjøpes inn eller installeres utstyr og/eller programvare i enheten uten at dette er godkjent av IKT-leder på forhånd.

Ved installering av ny programvare/app med ekstern systemansvarlig, forteller IKT-leder at programvaren/appen alltid sjekkes før den blir installert. Det er bestiller (systemansvarlig) som har ansvaret for dette, og i tilfeller der det er nødvendig, er det tett dialog med IKT-avdelingen. I dette ligger utarbeidelse av databehandleravtale og risiko- og sårbarhetsanalyse (ROS). Systemer som krever integrasjon om kommunens sine systemer, deltar IKT-avdelingen ved installering av ny programvare/app. IKT-leder forteller at han opplever at IKT-avdelingen er påkoblet tidlig i prosessen med anskaffelser av ny programvare/app.

Alle databehandleravtaler går via personvernombudet, ifølge flere av informantene. Personvernombudet gjennomgår avtalene og forutsetter at personvernregelverket etterleves, forteller personvernombudet. Blant annet forteller personvernombudet at kommunen har

sørget for at underleverandører ikke er etablert i ustabile land og risikoland. IKT-leder forteller at de fleste databehandleravtalene blir signert av kommunedirektør.

Regnearket (protokoll behandlingsansvarlige Vefsn kommune) som revisor har fått tilsendt inneholder referanse (saksnummer i Elements) til databehandleravtale. Referanse til Elements er registrert for 41 av systemene.

Videre forteller personvernombudet at det skal foreligge risiko- og sårbarhetsanalyse (ROS-analyse) i etterkant av databehandleravtaler. Personvernombudet gir tilbakemelding om at det skal utarbeides ROS-analyse, og at den skal ligge i behandlingsprotokollen. I ROS-analysen skal det vurderes om det er behov for tiltak. Personvernombudet har av og til bistått i utarbeidelse av ROS-analyser. Mal for utarbeidelse av ROS-analyse ligger i Compilo. Revisor fikk en demonstrasjon av denne fra sikkerhetsansvarlig.

3.3.3 Sikker IKT-arkitektur

Et av punktene i sikkerhetsstrategien for informasjonssikkerhet i dokumentet «Informasjonssikkerhet i Vefsn kommune» inneholder at kommunens informasjonssystem skal være konfigurert i samsvar med godkjent konfigurasjonskart. Det er kun utstyr og/eller program eiet/disponert av kommunen som skal inngå i informasjonssystemet. IKT-leder har ansvaret for å oppdatere endringene i konfigurasjonskartet med tilhørende beskrivelser, herunder innhente ledelsens godkjennelse av vesentlige endringer.

Sikkerhetsstrategien inneholder også punkt om systemteknisk sikkerhet og fysisk sikring. Inndeling av kommunens informasjonssystem skal gjenspeile skillet mellom behandlingen av sensitive og «ikke-sensitive» personopplysninger. I sikrede soner skal brukere kun gis begrenset tilgang til tjenester i øvrige deler av kommunens informasjonssystem og eksterne datanett. Utstyr skal fysisk sikres mot uautorisert tilgang når utstyret inngår i sikkerhetsbarrierer mellom informasjonssystemet forskjellige soner og mellom kommunens informasjonssystem og eksternt datanett.

IKT-leder forteller at to ansatte ved IKT-avdelingen har laget oversikt over fysisk struktur; her er det datarack (samling av datakabler fra ulike rom/kontor) som tilhører et patchpanel med tilhørende nettverksporter for lokasjonene i kommunen. Panelet gjør at de kan kontrollere alle tilkoblingene til enhetene, og nettlinjer kan ordnes og omorganiseres ved å koble om kabler.

Kommunen benytter innlogging med tofaktor autentisering til systemer med sensitiv informasjon og tjenester som benytter sikker løsning (eksempelvis barnevernstjenesten).

Eksterne enheter kan koble til gjestenettet. Pålogging via ukjent PC må benytte tofaktor autentisering innlogging. Møterommene har brukertilgang, men det er ikke tilgang til kjernen i kommunens nettverk, opplyser IKT-leder.

3.3.4 Sikkerhetsoppdatering

På systemer som IKT-avdelingen har ansvar for, forteller IKT-leder at det kjøres sikkerhetsoppdatering månedlig for PCene kommunen forvalter. Ved kritiske sikkerhetshull, kjøres oppdateringer uavhengig av faste tidspunkt. Revisor observerte under demonstrasjon av kommunens internkontrollsystem at månedlige sikkerhetsoppdateringer annonseres på kommunens intranett.

Når det gjelder andre systemer som kommunen ikke drifter, forteller IKT-leder at det er systemansvarlige som er ansvarlig for oppdatering av systemene. Det er leverandør som sørger for oppdateringene, opplyser IKT-leder om.

Rutinehåndboken for elektroniske meldinger innenfor helse, har en egen rutine for ny versjon/oppdatering av fagsystemet. Ansvarlig for dette er databehandlingsansvarlig ved IT-avdelingen, ifølge rutinen. Krav/aktiviteter er spesifisert i rutinen med frist og oversikt over hvem som er ansvarlig. Systemansvarlig for CosDoc opplyser om at det er IKT-avdelingene som sørger for oppdateringer av deres systemer. Dette gjenspeiler også rutinen, der ansvaret er lagt til IT-avdelingen i samråd med systemansvarlig.

3.3.5 Sikkerhetskopiering

IKT-leder forteller om kommunens rutiner for sikkerhetskopiering (backup). Rutinene sørger for at det skjer daglig, ukentlig, månedlig og årlig sikkerhetskopiering. I tillegg tas det inkrementell backup[12] av databaser hvert femte minutt. Dataene som ligger i backup er ikke mulig å endres, men kan slettes. Backup slettes ikke opplyser IKT-leder om, men overskrives av ny backup. I tillegg gjennomføres det sikkerhetskopiering som lagres fysisk i et avlåst, sikret bygg der kun autorisert personell har tilgang.

[12] En inkrementell backup/sikkerhetskopi tar kun sikkerhetskopi av endringer siden forrige fullstendige sikkerhetskopi.

3.3.6 Revisors vurdering

Kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.

Revisor vurderer kriteriet som delvis oppfylt.

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 kvalitetssikrer arbeidet gjennom at personvernombudet leser gjennom og kommer med innspill på databehandleravtale, samt at IKT-avdelingen er påkoblet i prosessen. Revisor er ikke sikker på hvilken rutine IKT-avdelingen har i å vurdere selve programvaren. NSM sitt grunnprinsipp om å ivareta sikkerhet i anskaffelsesprosesser handler om at dersom det anskaffes IKT-produkter og tjenester som har svak sikkerhet eller som ikke er integrert med kommunens øvrige arkitektur og eksisterende produkter, kan dette øke sårbarheten og redusere sikkerhetsnivåene i IKT-systemet.

Kommunen bør etablere og dokumentere en sikker IKT-arkitektur.

Revisor vurderer kriteriet som delvis oppfylt.

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, som NSM skriver i sine grunnprinsipper. Kommunen har ikke fått på plass et godkjent konfigurasjonskart i henhold til sin egen prosedyre som revisor vurderer som en svakhet. Konfigurasjonskart kan bidra til å dokumentere utstyr og programmer, og hvordan disse henger sammen for å vurdere kommunens behov for tilfredsstillende nivå av informasjonssikkerhet.

Kommunen bør ha sentral styring med sikkerhetsoppdateringer.

Revisor vurderer kriteriet som i hovedsak oppfylt.

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. Oppdateringer knyttet til andre system, er det systemansvarlig som er ansvarlig for.

Kommunen må ha en plan for sikkerhetskopiering og ta sikkerhetskopier.

Revisor vurderer kriteriet som oppfylt.

Revisor vurderer at Vefsn kommune har en praksis for sikkerhetskopiering, og tar sikkerhetskopier.

3.4 Oppdage

3.4.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

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

Utledningen av revisjonskriteriene finnes i vedlegg 1.

3.4.2 Overvåke systemene

IKT-leder har ansvaret for å overvåke bruken av kommunens informasjonssystemer med tanke på sikkerhetsbrudd og forsøk på uautorisert tilgang internt og/eller eksternt ifølge dokumentet «Informasjonssikkerhet i Vefsn kommune».

Når det gjelder overvåkning av sikkerheten i kommunen benytter kommunen et program til å overvåke feil med hardware komponenter, eksempelvis feil som lite diskplass, feil på disker og Central Processing Unit (CPU) – prosessoren til en PC, opplyser IKT-leder.

Kommunen er medlem av HelseCert. HelseCert er en tjeneste for norske kommuner som varsler angrep og svakheter som kommer utenfra for kommunene. HelseCert gjennomfører blant annet jevnlig sikkerhetsskanning av helsenett som inkluderer sårbarhetsskanning, portskanning og statusrapport e-postsikkerhet.[13] HelseCert informerer fortløpende ved kritiske hendelser og svakheter ifølge IKT-leder. Revisor har spurt hvem som følger opp loggene som kommer fra HelseCert. Til det svarer IKT-leder at de sjekker loggene selv ved mistanke.

Kommunen har ikke et system som overvåker for eksempel om ansatte trykker på lenker eller eposter som går ut av kommunen, opplyser IKT-leder.

[13] https://www.nhn.no/tjenester/helsecert

For helse og bruk av CosDoc beskriver rutinehåndboken for elektronisk meldingsutveksling rutine for hendelsesregistering og avdekking av uautorisert bruk av CosDoc. Formålet er å avdekke uautorisert bruk eller forsøk på uautorisert bruk av CosDoc. Ifølge rutinen skal det ukentlig kjøres logger i CosDoc for å avdekke misbruk av innsynsrett i pasientjournaler, og det er systemansvarlig som har ansvaret. Videre skal bruk av systemene som ikke er forutsatt meldes inn som avvik.

3.4.3 Inntrengningstester

IKT-leder opplyser om at kommunen ikke har hatt tid og ressurser til å gjennomføre inntrengingstester.

3.4.4 Revisors vurdering

Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen.

Revisor vurderer kriteriet som ikke oppfylt.

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. NSM skrier at målet med å etablere sikkerhetsovervåkning for sine IKT-systemer og samle inn relevant data er for å oppdage sikkerhetshendelser tidlig, vurdere skadeomfanget og hendelsens karakter og forstå hendelsesforløpet. Mangelfull overvåkning kan gjøre at angripere skjuler sin tilstedeværelse, handlinger og aktiviteter i kommunens systemer.

Kommunen bør gjennomføre inntrengningstester.

Revisor vurderer kriteriet som ikke oppfylt.

Kommunen gjennomfører ikke inntrengningstester.

3.5 Håndtere og gjenopprette

3.5.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen bør ha en plan for hendelseshåndtering.
- Kommunen må ha en plan for gjenoppretting.

Utledningen av revisjonskriteriene finnes i vedlegg 1.

3.5.2 Hendelseshåndtering

Vefsn kommune har en overordnet beredskapsplan som er oppdatert av kommunedirektøren 7. februar 2024. Overordnet beredskapsplan inneholder blant annet organisering av beredskapsledelsen under en hendelse. Det er den enkelte hendelse som er avgjørende for sammensetningen av beredskapsledelsen. Under roller og oppgaver kommer det frem at kommunen har en egen beredskapsleder[14] som har oppgaven med å være kommunedirektørens operative støttefunksjon. I planen står det at IKT-avdelingen skal alltid varsles og innkalles ved behov.

Revisor har fått tilsendt beredskapsplan for IT, men denne er ikke godkjent av kommunedirektør. Planen beskriver blant annet roller og ansvar. Ifølge planen består kriseledelse av «ordfører, rådmann og beredskapsansvarlig». Videre står det at:

> «Hendelseshåndteringsteamet er en arbeidsgruppe som er operativt ansvarlig for å gjennomføre tekniske tiltak i henhold til hendelseshåndteringsplanen. Hendelseshåndteringsteamet rapporterer til krisestaben. Hendelseshåndteringsteamet kan være internt personell eller en ekstern SOC.»

Beredskapsplanen inneholder videre et utvalg av uønskede hendelser innenfor IT. Hver hendelse er beskrevet og det er gjort en risikovurdering. På bakgrunn av denne er det utarbeidet sikkerhetstiltak og respons. Sikkerhetstiltak viser gjerne til ulike policyer eller service- og supportavtale[15], mens respons sier noe om håndteringen av hendelsen. I håndteringen refereres det til hendelseshåndteringsplan eller avtale med en SOC-partner. Revisor har ikke fått tilsendt eller fått informasjon om at det finnes en hendelseshåndteringsplan. IKT-leder opplyser om at de jobber med å få dette opprettet.

Ved en hendelse i kommunen, forteller IKT-leder at de i hovedsak er selvhjulpen. Vefsn kommune har ingen ekstern avtale med for eksempel en SOC-tjeneste som bistår kommunen ved en eventuell hendelse.

---

[14] IKT-leder opplyser om at kommunalsjef for infrastruktur er beredskapsleder.

[15] Revisor har fått tilsendt foreløpig utkast til ulike policyer, men velger å ikke omtale de nærmere her

Revisor har spurt systemansvarlig for Elements hva de gjør dersom systemet er nede. Rutinene for Elements er at posten i kommunen blir stemplet og lagt til side. Posten vil bli scannet i etterkant. Dersom kommunen mottar eksempelvis viktig informasjon som haster å få videre, vil dette bli overlevert på papir. Systemansvarlig forteller at det gjøres vurderinger i hvert enkelt tilfelle. Det er ikke skriftlige rutiner for slik hendelse.

På helse, forteller systemansvarlig for CosDoc at alle avdelingene skal ha en medisinliste i en perm som er innelåst på avdelingene, for eksempel på medisinrommet. Medisinromsdørene er alltid låst, og det er kun helsepersonell som er har tilgang. Dørene er utstyr med nøkkelkort, samt at noen dører har kode i tillegg. Ved et strømbrudd kan dørene låses opp ved en nødnøkkel som er innelåst i et annet skap. Det er også rutiner for oppbevaring av medisinlister for papir for hjemmeboende.

Rutinehåndboken for elektronisk meldingsutveksling inneholder en rutine for nødprosedyre for alternativ drift. Formålet med rutinen er å sikre at virksomhetens behandling av helse- og personopplysninger ivaretas ved ikke-planlagt driftsstans i IKT-systemene. Rutinen inneholder en liste over krav/aktiviteter som må gjennomføres til hvilke frister og hvem som er ansvarlig. Det gjelder blant annet at legemiddelliste skrives ut fortløpende ved endringer. Dette skal gjøres kontinuerlig og det er avdelingsleder som er ansvarlig.

Sykehjemstjenesten, hjemmetjenesten og miljøterapitjenesten har en egen plan for kriseberedskap. Planen inneholder tiltak ved hendelser/scenario og hvem som er ansvarlig for gjennomføringen av tiltakene. Et av scenarioene er skade på kritisk infrastruktur, blant annet strømstans i institusjon og elektronisk pasientjournal ute av drift.

3.5.3 Plan for gjenoppretting

Beredskapsplanen for IT inneholder en systemoversikt. I oversikten er det lagt opp til en vurdering av hvor kritisk de enkelte systemene er for kommunen for å kunne identifisere hvilke systemer som er kritisk for kommunen for at de skal levere sine tjenester. Det er også gjort en vurdering av hvor langt tilbake i tid kommunen må kunne gjenopprette data etter en uforutsett hendelse; RPO (Recovery Point Objective). Dette uttrykker det maksimale datatapet kommunen tillater. PRO må sees i sammenheng med krav til sikkerhetskopiering og gjenoppretting. Det er også vurdert hvor raskt kommunen må kunne gjenoppta driften av systemene etter uforutsette hendelser; RTO (Recovery Time Objective). RTO beskriver maksimal tillatt tid det skal ta å gjenopprette systemene.

I systemoversikten er det gjort en slik vurdering for to av systemene; AD-kontrollere og nettverk og nettverkstjenester, der både RTO og PRO er vurdert til 24 timer.

Revisor har spurt IKT-leder om kommunen har en oversikt over hvilke systemer som er kritisk for at kommunen skal få levert sine tjenester og om dette er dokumenter. IKT-leder er usikker på om de har god dokumentasjon på dette, og at de prioritere system for helse og omsorg (CosDoc).

3.5.4 Revisors vurdering

Kommunen bør ha en plan for hendelseshåndtering

Revisor vurderer kriteriet som ikke oppfylt.

Vefsn 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. Nasjonal sikkerhetsmyndighets sitt grunnprinsipp om en hendelseshåndteringsplan handler om å ha et planverk for å ivareta behovet for virksomhetskontinuitet ved beredskap og kriser, for eksempel at datasystemene ikke er tilgjengelige. En beredskapsplan vil også bidra til å beskrive roller og ansvar i en hendelseshåndtering. 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.

Kommunen må ha en plan for gjenoppretting.

Revisor vurderer kriteriet som ikke oppfylt

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.

4 KONKLUSJONER OG ANBEFALINGER

4.1 Konklusjon

I denne forvaltningsrevisjonen har revisor undersøkt om Vefsn kommune har nødvendig informasjonssikkerhet. Det har vi gjort ved å belyse to problemstillinger.

På problemstillingen **om kommunen har etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket**, konkluderer revisor med at kommunen langt på veg har etablert et slikt styringssystem. Kommunen har et styringsdokument for informasjonssikkerhet med sikkerhetsmål og beskrivelse av sikkerhetsansvar og -organisering. Revisor vil også trekke fram at informasjonssikkerhet er inkludert i kommunens system for internkontroll. Revisor ser likevel en del svakheter i systemene for informasjonssikkerhet. Revisor mener at 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.

Videre konkluderer revisor med at det er en svakhet at overordna ROS og beredskapsplan ikke berører trusler som gjelder informasjonssikkerhet. Trusler mot informasjonssikkerhet er blant de største risikoene kommuner har stått overfor de siste tiårene. Revisor mener videre, at det kan stilles spørsmål ved den generelle opplæringen i organisasjonen i informasjonssikkerhet.

På problemstillingen **om kommunen har tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet**, konkluderer revisor med at kommunen langt på vei har slike tiltak. Revisor mener 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. 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.

4.2 Anbefalinger

Revisor anbefaler kommunedirektøren å sørge 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

KILDER

Datatilsynet. «Virksomheters plikter». Åpnet 14. mars 2025. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/.

Digitaliserings- og forvaltningsdepartementet. «Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)», 2004.

Justis- og beredskapsdepartementet. «Forskrift om virksomheters arbeid med forebyggende sikkerhet», 2018.

Justis- og beredskapsdepartementet. Lov om behandling av personopplysninger (personopplysningsloven), Pub. L. No. LOV-2018-06-15-38 (2018). https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=lov%20om%20behandling%20av%20personopplysninger.

Justis- og beredskapsdepartementet. «Lov om nasjonal sikkerhet (Sikkerhetsloven)», 2018.

KS. «Orden i eget hus - kommunedirektørens internkontroll», 2020. https://www.ks.no/globalassets/fagomrader/lokaldemokrati/internkontroll/Kommunedirektorens-internkontroll-veileder-F41-web.pdf.

KS og KPMG. «Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet», 2022. https://www.ks.no/contentassets/c019638eeb1e4972bac838e34c75dc47/-19-03185-6-Kommunedirektorens-verktoykasse-for-personvern-og-informasjonssikkerhet-1418678-2-1.pdf.

Nasjonal sikkerhetsmyndighet (NSM). «Grunnprinsipper for IKT-sikkerhet», 2024.

Nasjonal sikkerhetsmyndighet (NSM). «Veileder i sikkerhetsstyring», 2020. https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-sikkerhetsstyring/om-denne-veilederen/.

VEDLEGG 1 – UTLEDNING AV REVISJONSKRITERIER

Ifølge forskrift om kontrollutvalg og revisjon (§15) skal det etableres revisjonskriterier for gjennomføring av forvaltningsrevisjon. Revisjonskriterier er de krav og forventninger som forvaltningsrevisjonsobjektet skal revideres/vurderes i forhold til. Disse kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. Slike autoritative kilder kan være lov, forskrift, forarbeider, rettspraksis, politiske vedtak (mål og føringer), administrative retningslinjer, samt statlige føringer og praksis. I denne forvaltningsrevisjonen har vi benyttet oss av følgende kilder til revisjonskriterier:

- Lov om nasjonal sikkerhet (Sikkerhetsloven)[16]
- Lov om behandling av personopplysninger (Personopplysningsloven)[17]
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)[18]
- Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetsikkerhetsforskriften)[19]
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet[20]
- NMS' grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet[21]
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet[22]

Problemstilling 1: Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket

Overordnet styringssystem og rammeverk

Sikkerhetsloven stiller generelle krav til forebyggende sikkerhetsarbeid i kapittel 4. Sikkerhetsstyring er hjemlet i § 4-1; forebyggende sikkerhetsarbeid skal være en del av

[16] Justis- og beredskapsdepartementet, «Lov om nasjonal sikkerhet (Sikkerhetsloven)».

[17] Justis- og beredskapsdepartementet, Lov om behandling av personopplysninger (personopplysningsloven).

[18] Digitaliserings- og forvaltningsdepartementet, «Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)», 2004.

[19] Justis- og beredskapsdepartementet, «Forskrift om virksomheters arbeid med forebyggende sikkerhet», 2018.

[20] Nasjonal sikkerhetsmyndighet (NSM), «Veileder i sikkerhetsstyring».

[21] Nasjonal sikkerhetsmyndighet (NSM), «Grunnprinsipper for IKT-sikkerhet», 2024.

[22] Datatilsynet, «Virksomheters plikter», åpnet 14. mars 2025, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/.

virksomhetens styringssystem. Virksomhetsikkerhetsforskriften definerer i § 3 kravet om at virksomheter som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at virksomheten oppfyller kravene gitt i eller med hjemmel i loven.

Nasjonal sikkerhetsmyndighets veileder i sikkerhetsstyring skriver at sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier. Skjermingsverdige verdier er definert i sikkerhetslovens § 6-1 første ledd: Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.

Videre skriver veilederen at sikkerhetsstyring omfatter alle aktiviteter som har betydning for det forebyggende sikkerhetsarbeidet og skal gjennomføres planlagt og systematisk i form av et sikkerhetsstyringssystem som omfatter planlegging, etablering, gjennomføring og forbedring av det forebyggende sikkerhetsarbeidet. Utformingen av styringssystemet for sikkerhet skal omfatte følgende prinsipper:

- Risikostyring
- Sikkerhetsledelse
- Sikkerhetsorganisering
- Sikkerhetstiltak og prosedyrer
- Forhold til andre virksomheter
- Sikkerhetsoppfølging
- Sikkerhetsdokumentasjon

Datatilsynet anbefaler i sin veileder om virksomhetens plikter at anerkjente standarder, rammeverk og veiledere som beskriver styringssystem for informasjonssikkerhet benyttes.

Sikkerhetsmål og sikkerhetsstrategi

Forskriften fastsetter krav om sikkerhetsmål i § 5. Virksomheten skal fastsette hvordan kravene til et forsvarlig sikkerhetsnivå skal oppfylles og kriterier og å evaluere om kravene er oppfylt. eForvaltningsforskriften omhandler internkontroll på informasjonssikkerhetsområdet for forvaltningsorgan i § 15. Første ledd krever at mål og strategier for informasjonssikkerhet er beskrevet (sikkerhetsmål og sikkerhetsstrategi). Dette skal danne grunnlaget for forvaltningsorganets internkontroll på området for informasjonssikkerhet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller

instruks. Kravene i personvernforordningen vil være aktuelle å innarbeide i en slik sikkerhetsstrategi.

Datatilsynet skriver at sikkerhetsstrategien skal omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Dette gjelder blant annet fordeling og avklaring av arbeidsoppgaver mellom ledelse og driftspersonell, men også beslutning om eventuelt å ta i bruk eksterne leverandører i sikkerhetsarbeidet. Videre skal sikkerhetsstrategien gjøre rede for organisatoriske og tekniske strategiske valg. Strategien beskriver hvilke virkemidler virksomheten velger å bruke for å nå målene.

Informasjonsverdier

I KS`veileder, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet heter det at all informasjonen kommunen eier og behandler har en verdi. Verdien varierer ut fra typen informasjon og hvilken type virksomhet informasjonen tilhører. Informasjon i denne sammenhengen er alt fra kunnskap, personopplysninger, forretningshemmeligheter, beregningsmodeller, informasjon om hvordan saksbehandlingen skal gjennomføres, IKT-systemer hvor informasjon blir behandlet, teknisk infrastruktur mv.

Sikkerhetsorganisasjon

Jamfør sikkerhetsloven § 4-1 er det er virksomhetens leder som har ansvaret for det forebyggende sikkerhetsarbeidet. I forskriften om virksomhetens sikkerhet, framgår det i § 4 krav om styringsdokument. Leder av virksomheten skal fastsette et styringsdokument som beskriver hvilke deler av sikkerhetsloven som gjelder for virksomheten, roller og ansvar i virksomhetens forebyggende sikkerhetsarbeid og prinsipper for virksomhetens sikkerhetsarbeid. Styringsdokumentet skal gjøres kjent og tilgjengelig for blant annet alle ansatte. Virksomhetsforskriften § 6 definerer videre krav til roller og ansvar for det forebyggende sikkerhetsarbeidet. Det er leder sitt ansvar å fordele roller og ansvar, og at disse gjøres kjent i virksomheten.

Internkontroll

Internkontroll er hjemlet i kommuneloven § 25, der det står at internkontrollen skal være systematisk og tilpasset virksomhetens størrelse, egenart, aktiviteter og risikoforhold.

Kommunedirektøren er ansvarlig for internkontrollen og skal:

a. utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering

b. ha nødvendige rutiner og prosedyrer

c. avdekke og følge opp avvik og risiko for avvik

d. dokumentere internkontrollen i den formen og det omfanget som er nødvendig

e. evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Andre ledd i § 15 i eForvaltningsforskriften krever at det skal være etablert internkontroll på området for informasjonssikkerhet. Internkontrollen skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være integrert som en del av virksomhetens helhetlige styringssystem. Tredje ledd § 15 krever at omfang og innretning på internkontroll skal være tilpasset risiko. I fjerde ledd bokstavene a til h, § 15, gis det eksempler på hvilke forhold sikkerhetsstrategien og internkontrollen bør adressere, herunder prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

Risikovurderinger

Sikkerhetsloven § 4-2 krever at virksomheten skal regelmessig gjennomføre vurdering av risiko. Vurderingen danner grunnlaget for iverksetting av forebyggende sikkerhetstiltak. Videre skal virksomheten kartlegge, som en del av vurderingen, om hvilke virksomheter den er avhengig av for å fungere som den skal. Vurderingen skal gjennomgås jevnlig og om nødvendig revideres. Kravet om vurdering av risiko er videre utdypet i virksomhetsikkerhetsforskriften § 12. Forskriften skriver i andre ledd at behovet for å gjennomføre en ny helhetlig vurdering av risikoen skal vurderes årlig.

Personopplysninger

Personopplysningsloven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven gjennomfører EUs personvernforordning i norsk rett. Personopplysningsloven er bygget på noen grunnleggende prinsipper, og alle som behandler personopplysninger må følge disse prinsippene.

Datatilsynet har laget informasjon om pliktene en virksomhet har etter personvernregelverket. En av pliktene Datatilsynet referer til er vurdering av personvernkonsekvenser (DPIA – Data Protection Impact Assessment) (artikkel 35 i personopplysningsloven). Artikkel 35 krever at virksomheten gjennomfører en vurdering av personvernkonsekvenser ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter. Datatilsynet skriver følgende om DPIA:

> «En vurdering av personvernkonsekvenser er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak.»

DIPA skal som minimum inneholde:

> a) En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen.
>
> b) En vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene.
>
> c) En vurdering av risikoene for de registrertes rettigheter og friheter
>
> d) De planlagte tiltakene for å håndtere risikoene og for å påvise at forordningen overholdes.

En av pliktene er at alle virksomheter som behandler personopplysninger, skal føre protokoll over behandlingsaktivitetene de har ansvar for (artikkel 30 i personopplysningsloven). Protokollen skal inneholde formålet med behandlingen, hvilke kategorier personopplysninger kommunen behandler, tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Dersom det er aktuelt, skal eventuelle databehandlere så oppført i protokollen.

Datatilsynet skriver at personvernforordningen skiller mellom begrepene behandlingsansvarlig og databehandler. Den behandlingsansvarlige bestemmer over personopplysningene, mens databehandleren opptrer på vegne av den behandlingsansvarlige. Databehandleren kan derfor bare behandle personopplysninger etter instruks fra den behandlingsansvarlige.

Opplæring

Sikkerhetsloven definerer i § 4-1 at virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. Kravet om ressurser og kompetanse er videre utdypet i virksomhetsforskriften § 7. Forskriften krever blant annet at de ansatte som får tilgang til skjermingsverdige verdier, får tilstrekkelig kompetanse om sikkerhet og kartlegge at personene kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser.

Veilederen fra NSM skriver at riktig kompetanse oppnås og opprettholdes gjennom planmessig opplæring, kvalifisering og kompetansevedlikehold.

Datatilsynet skriver at målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt. Brukerne må være gitt muligheten til å etterleve dette i ditt daglige arbeid gjennom tilpasset opplæring ut ifra behov. Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.

Hendelser

Virksomhetsforskriften § 8 sier at ved sikkerhetstruende virksomhet eller avvik fra styringssystemet for sikkerhet skal en virksomhet gjennomføre umiddelbare tiltak for å redusere skadeomfanget og gjenopprette et forsvarlig sikkerhetsnivå. Virksomheten skal vurdere konsekvensene av den sikkerhetstruende virksomheten eller avviket.

NSM sine grunnprinsipper (versjon 1) sier at etter en uønsket hendelse det det forebyggende sikkerhetsarbeidet i virksomheten evalueres. Virksomheten må forsikre seg om at tiltakene som er etablert fungerer etter hensikten og vurdere om hendelsen ble håndtert tilfredsstillende.

NSM skriver at dette er viktig fordi:

> «Når en hendelse er ferdig håndtert og akseptabelt sikkerhetsnivå gjenopprettet, er det viktig at virksomheten hurtig identifiserer og lærer fra det inntrufne og sørger for at konklusjoner blir gjennomgått og tatt tak i. Dersom dette ikke gjøres vil kunnskap og erfaring forsvinne, og man kan gjøre de samme feilene om igjen neste gang en uønsket hendelse oppstår. Det kan være at det oppdages nye sårbarheter, eller behov for nye eller forbedrede sikringstiltak som kan forhindre at fremtidige situasjoner oppstår.»

På bakgrunn av redegjørelsen over, er følgende revisjonskriterier utledet for styringssystem:

- Kommunen skal ha et overordna, oppdatert styringssystem for informasjonssikkerhet som angir sikkerhetsmål, sikkerhetsstrategi og kommunens informasjonsverdier
- Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår.
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.
- Kommunen skal føre protokoll over hvilke personopplysninger de behandler.

- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.
- Kommunen bør evaluere og lære av hendelser.

Problemstilling 2: Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

Nasjonal sikkerhetsmyndighet har utgitt en veileder om grunnprinsipper for IKT-sikkerhet for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene fokuserer på teknologiske og organisatoriske tiltak, og hovedfokuset er på tilsiktende handlinger.

Grunnprinsippene er delt inn i fire kategorier og er gjengitt i tabellen under.

1. Identifisere og kartlegge	**2. Beskytte og opprettholde**
Kartlegge styringsstrukturer, leveranser og understøttende systemer Kartlegge enheter og programvare Kartlegge brukere og behov for tilgang	Ivareta sikkerhet i anskaffelses- og utviklingsprosesser Etablere en sikker IKT-arkitektur Ivareta en sikker konfigurasjon Beskytte virksomhetens nettverk Kontroller dataflyt Ha kontroll på identiteter og tilganger Beskytt data i ro og i transitt Beskytt e-post og nettleser Etabler evne til gjenoppretting av data Integrer sikkerhet i prosess for endringshåndtering
3. Oppdage	**4. Håndtere og gjenopprette**
Oppdage og fjerne kjente sårbarheter og trusler Etablere sikkerhetsovervåkning	Forberede virksomheten på håndtering av hendelser Vurdere og klassifisere hendelser

Analysere data fra sikkerhetsovervåkning Gjennomfør inntrengingstester	Kontrollere og håndtere hendelser Evaluere og lære av hendelser

Identifisere og kartlegge

NSM skriver at kartlegging av enheter og programvare er viktig for å få oversikt over hva som befinner seg i kommunen. Det er viktig at kommunen selv får oversikt over enheter, programvare og deres sårbarheter før angripere gjør det.

Videre skriver NSM at risikobildet må vurderes knyttet opp til valget mellom sikkerhet og behovet for leveranser til kommunen. Det kan hende at kommunen må godta enheter med lavere sikkerhetsnivå enn ønsket, og det er derfor viktig at kommunen er bevisst på strategier som velges og vurderer de funksjonelle behovene opp mot risiko. Anbefalt tiltak fra NSM er å kartlegge enheter og programvare.

Det er også viktig at kommunen har oversikt over hvilke brukergrupper, brukere og tilgangsbehov som finnes i en kommune. En angriper har ofte som mål å økte tilgangen ved et angrep på informasjonssystemet. Mange brukere kan ha tilganger og rettigheter til systemer og tjenester de egentlig ikke har behov for. Derfor bør tilganger og rettigheter begrenses slik at skaden fra en potensiell angriper eller utro ansatt reduseres. Derfor bør kommunen kartlegge brukere og behov for tilgang.

Utledet revisjonskriterier:

- Kommunen må ha en oversikt over enheter i IKT-systemet.
- Kommunen bør ha en oversikt over programvare.
- Kommunen må ha et system for styring av tilganger.

Beskytte og opprette

NSM har et prinsipp som sier at sikkerheten i anskaffelse- og utviklingsprosesser må ivaretas. Målet med prinsippet er å minimere risiko for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter.

Et av prinsippene under denne kategorien er å etablere en sikker IKT-arkitektur. Et IKT-system består av mange sikkerhetsfunksjoner og ulike IKT-produkter fra ulike produsenter som skal

fungere godt og sikkert sammen. Hvis ikke så kan dette økte sårbarheten og som en angriper kan utnytte. Videre skriver NSM at drift og sikkerhetskonfigurasjon bør skje sentralt og likt per type enhet, hvis ikke økes risikoen for dobbeltarbeid, menneskelige feil og flere sårbarheter. IKT-systemet bør videre deles opp i forskjellige deler avhengig av tillitsnivå for å begrense risiko.

Under prinsippet om å ivareta en sikker konfigurasjon kommer NSM med et anbefalt tiltak om å etablere et sentralt styrt regime for sikkerhetsoppdatering. I dette ligger det blant annet at kommunen bør installere sikkerhetsoppdatering så fort som mulig. Videre bør kommunen ha en prioriteringsliste for oppdateringer og etablere en rutine med klare ansvarsforhold for hvor ofte oppdateringer skal utføres og hvem som er ansvarlig dersom en oppdatering ikke kan gjennomføres eller må utsettes.

NSM skriver at et av prinsippene er å etablere en metode for sikkerhetskopiering og gjenoppretting av kritiske data for å hindre tap. Et av de anbefalte tiltakene er å lage en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata.

Utledet revisjonskriterier:

- Kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.
- 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

NSM har et prinsipp som omhandler etablering av sikkerhetsovervåkning for å overvåke og samle inn relevante data for å oppdage sikkerhetshendelser og legge et grunnlag for å analysere data. Dette for at kommunen kan oppdage sikkerhetshendelser tidlig som mulig for å minimere skadeomfang eller forhindre hendelser. Det er viktig at kommunen har tilgang på tilstrekkelig data siden det kan være avgjørende for at kommunen skal gjenopprette normaltilstand og hindre gjentagelse av en hendelse. NSM anbefaler derfor at kommunen etablerer sikkerhetsovervåkning.

Videre anbefaler NSM at kommunen analyserer data fra sikkerhetsovervåkningen. Gjennom analyse av sikkerhetsrelevante data kan kommunen oppdage aktiviteter som påvirker informasjonssystemer, data og tjenester. NSM skriver at systematisert prosessering, gjennom sammenstilling og analyse av innhentet data vil bidra til å øke sannsynligheten for å avdekke hendelser.

Et prinsipp til under kategorien oppdage, er at kommunen bør gjennomføre inntrengningstester. Kommunen bør jevnlig teste egen forsvarsevne for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Angripere utnytter ofte svakheter i virksomhetens rutiner.

Utledet revisjonskriterier:

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

Håndtere og gjenopprette

For å forberede kommunen på håndtering av hendelser anbefaler NSM at kommunen etablerer et planverk for hendelseshåndtering. Uten en plan og en prosess for hendelseshåndtering vil det være vanskelig for kommunen å begrense skaden og gjenopprette normal tilstand.

Ved en hendelse er det viktig at kommunen håndtere hendelsen korrekt og med riktige ressurser slik at spredning og konsekvenser minimeres og normaltilstand opprettholdes eller gjenopprettes effektivt. For å få til dette er det viktig at kommunen har en plan for gjenoppretting som iverksettes i løpet av eller i etterkant av hendelsen.

Utledet revisjonskriterier:

- Kommunen bør ha en plan for hendelseshåndtering.
- Kommunen må ha en plan for gjenoppretting.

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no