RAPPORT

IKT-sikkerhet i FARTT

For

Tynset, Tolga, Alvdal og Rendal kommune

6. november 2023

BDO
tett på

INNHOLD

1 SAMMENDRAG

Kontrollutvalget i Tynset kommune har bestilt en forvaltningsrevisjon innen IKT-sikkerhet og personvern. Alvdal, Rendalen og Tolga har underveis i revisjonen knyttet seg til revisjonen. Formålet med forvaltningsrevisjonen har vært å gi eierkommunene en ekstern vurdering av IKT-sikkerheten hos FARTT, og å bidra til å identifisere forbedringsområder som må utbedres for at FARTT skal ha et tilfredsstillende IKT-sikkerhetsnivå.

Det er fastsatt fem problemstillingen for forvaltningsrevisjonen:

1. Styrer selskapet informasjonssikkerheten på en tilfredsstillende måte?
2. Blir sikkerhetsrisikoer identifisert og håndtert?
3. Blir informasjon og informasjonssystemer beskyttet iht. beste praksis?
4. Hvordan oppdages avvik og mulige trusler mot virksomheten?
5. Blir hendelser håndtert på en tilfredsstillende måter?

Det er BDOs samlede vurdering at FARTT har hatt et økende fokus på IT-sikkerhet, men at det gjenstår vesentlige forbedringer for å kunne stadfeste at FARTT har et tilfredsstillende IKT-sikkerhetsnivå.

Gjennomgående for revisjonen er at FARTT har innført forbedringer det siste året, men at det fremdeles er en del avvik sett opp mot NSMs grunnprinsipper for IKT-sikkerhet og anerkjent beste praksis.

Disse avvikene innebærer at FARTT og eierkommunene er sårbare for cyberangrep, og at det ved en større hendelse kan ta lengre tid enn nødvendig å oppdage angrepet, begrense og håndtere skadeomfanget, og gjenopprette systemene.

2 INNLEDNING

2.1 INFORMASJON OM BESTILLINGEN

Kontrollutvalget i Tynset kommune bestilte våren 2023 en forvaltningsrevisjon av IKT-sikkerhet og personvern. Når avtalen med Tynset kommune ble inngått var det på bakgrunn av at det hadde pågått en prosess mot kontrollutvalgene i eierkommunene, hvor tre av de andre eierkommunene hadde gitt beskjed om at de ønsket å delta. Alvdal, Rendalen og Tolga kommune vedtok i mars 2023 at de ville være en deleier av forvaltningsrevisjonen. BDO har forholdt seg til Tynset kommune som oppdragsgiver. Formålet med forvaltningsrevisjonen har vært å gjøre en evaluering av IKT-sikkerheten i det interkommunale selskapet IKT Fjellregionen IKS (heretter omtalt som FARTT).

IKT-sikkerhetsområdet har vært trukket frem som et prioritert område for forvaltningsrevisjon i Tynset kommune over tid. I risiko- og vesentlighetsvurderingen for 2020 gjort for kontrollutvalget, skrives det følgende om IKT-sikkerhetsområdet:

> *IKT er et viktig virkemiddel for å effektivisere offentlig sektor. Det kan være grunn til å se på hvilke ressurser som blir benyttet til utviklingsarbeid, og hvor høyt strategisk bruk av IKT blir prioritert.*
>
> *I 2018 fikk Norge ny personopplysningslov. Loven består av nasjonale regler og EUs personvernforordning (GDPR - General Data Protection Regulation). Forordningen er et sett regler som gjelder for alle EU/EØS-land. Endringer i lovverket, og at temaer knyttet til informasjonssikkerhet og personvern er viktige områder, innebærer at IKT-sikkerhet kan være et aktuelt tema for en forvaltningsrevisjon.*
>
> *Andre aktuelle områder kan være IKT-sikkerhet i forhold til IKT-drift generelt. For Tynset kommune driftes IT-systemene av IKT Fjellregionen IKS. Organisering av IT-funksjoner i et interkommunalt selskap innebærer større avstand og mindre innflytelse på drift og utvikling fra kommunen enn om kommunen hadde driftet systemene selv. Dette kan innebære både fordeler og ulemper for Tynset kommune.*
>
> *Ettersom en vesentlig del av et forvaltningsrevisjonsprosjekt vil måtte rettes mot IKT Fjellregionen IKS bør det vurderes et samarbeidsprosjekt med de andre eierkommunene. Det vil også være hensiktsmessig å gjennomføre en eierskapskontroll samtidig, ettersom temaet for forvaltningsrevisjon har nær tilknytning til kommunens forvaltning av eierskapet i selskapet.*
>
> *Risikoen vurderes å være middels mens vesentligheten er vurdert til høy.*

2.2 FORMÅL OG PROBLEMSTILLINGER

Oppdraget til BDO er en forvaltningsrevisjon, og omfatter ikke eierskapskontroll. Revisjonen er gjennomført etter RSK001 – Standard for forvaltningsrevisjon.

Den viktigste målsettingen med revisjonen har vært å gi eierkommunene en ekstern vurdering av IKT-sikkerheten hos *IKT Fjellregionen IKS* (FARTT), og å bidra til å identifisere forbedringsområder som må utbedres for at FARTT skal ha et tilfredsstillende IKT-sikkerhetsnivå. Videre har revisjonen hatt som mål å utarbeide anbefalinger og tiltak.

I planleggingsfasen av oppdraget ble det i samarbeid med kontrollutvalget i Tynset kommune utarbeidet fem problemstillinger som skulle dekke kontrollutvalgets bestilling. Disse problemstillingene danner grunnlaget for de spørsmålene som eierkommunene ønsker besvart:

Nr.	Problemstillinger
1.	Styrer selskapet informasjonssikkerheten på en tilfredsstillende måte?
2.	Blir sikkerhetsrisikoer identifisert og håndtert?
3.	Blir informasjon og informasjonssystemer beskyttet iht. beste praksis?
4.	Hvordan oppdages avvik og mulige trusler mot virksomheten?
5.	Blir hendelser håndtert på en tilfredsstillende måte?

For å besvare problemstillingene har forvaltningsrevisjonen tatt utgangspunkt i revisjonskriterier hentet fra anerkjente standarder, herunder Nasjonal Sikkerhetsmyndighets (NSMs) grunnprinsipper for IKT-sikkerhet. Revisjonen har hatt hovedfokus på IKT-sikkerhet, men har også omfattet personvern i relasjon til god informasjonssikkerhet der dette er relevant.

Revisjonskriteriene for hver enkelt problemstilling er beskrevet i kapittel 2.3 nedenfor, mens observasjoner, vurderinger og konklusjoner inngår i kapittel 3 – 7.

2.3 REVISJONSKRITERIER

Revisjonskriterier er en samlebetegnelse på de normene og standardene som er relevante på området i en gitt revisjon. Revisjonskriteriene sin funksjon er å gi det normative grunnlaget for analysen. Ved utarbeidelse av prosjektplanen ble følgende kilder trukket frem som grunnlag for revisjonskriteriene:

- Lov om kommuner og fylkeskommuner (kommuneloven)
- Forskrift om kommunal beredskapsplikt
- NSMs grunnprinsipper for IKT-sikkerhet 2.0
- ISO/IEC 27001:2017 Ledelsessystemer for informasjonssikkerhet (heretter omtalt som ISO/IEC 27001)
- Digitaliseringsdirektoratet (2020), Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner, Kunnskapsgrunnlag – En dokumentstudie.

Revisjonskriteriene som er brukt for denne revisjonen er i hovedsak basert på NSMs grunnprinsipper for IKT-sikkerhet 2.0. Dette er et sett med prinsipper for hvordan IKT-systemer bør sikres for å beskytte verdier og leveranser. NSMs grunnprinsipper er et anerkjent rammeverk for beste praksis i Norge, og benyttes av en rekke virksomheter i både offentlig og privat sektor. Revisors erfaring og beste praksis er lagt til grunn ved vurdering, tilpassing og avgrensing av kontrollene for revisjonens formål.

Problemstilling 1: Styrer selskapet informasjonssikkerheten på en tilfredsstillende måte?

Dette er kontrollert gjennom besvarelse av følgende revisjonskriterier:

- Selskapet har etablert et styringssystem for informasjonssikkerhet.
- Selskapet har definert roller og ansvar knyttet til arbeid med informasjonssikkerhet.
- Selskapet har utarbeidet styrende dokumenter for informasjonssikkerhet.

Problemstilling 2: Blir sikkerhetsrisikoer identifisert og håndtert?

Dette er kontrollert gjennom besvarelse av følgende revisjonskriterier:

- Selskapet har kartlagt alle enheter og programvare som er i bruk.
- Selskapet har kontroll på alle identiteter og tilganger.
- Selskapet har utarbeidet, og reviderer jevnlig, risiko- og sårbarhetsanalyse av IKT-systemene.

Problemstilling 3: Blir informasjon og informasjonssystemer beskyttet iht. beste praksis?

Dette er kontrollert gjennom besvarelse av følgende revisjonskriterier:

- Selskapet har etablert et regime for sikker IKT-arkitektur og konfigurasjon.
- Selskapet har oversikt og kontroll over hele livsløpet til de tjenestene som forvaltes på vegne av kommunene og som er tjenesteutsatt.
- Selskapet har en plan for regelmessig sikkerhetskopiering av all virksomhetsdata for kommunene.

Problemstilling 4: Hvordan oppdages avvik og mulige trusler mot virksomheten?

Dette er kontrollert gjennom besvarelse av følgende revisjonskriterier:

- Selskapet har etablert sikkerhetsovervåkning av utvalgte deler av IKT-systemet.
- Selskapet har rutiner for å oppdage og fjerne kjente sårbarheter og trusler.
- Selskapet har gjennomført inntrengningstester på utvalgte IKT-systemer.

Problemstilling 5: Blir hendelser håndtert på en tilfredsstillende måte?

Dette er kontrollert gjennom besvarelse av følgende revisjonskriterier:

- Selskapet har et planverk for hendelseshåndtering og som revideres jevnlig.
- Selskapet har gjennomført regelmessige øvelser på informasjonssikkerhetshendelser.
- Selskapet har evaluert og implementert tiltak etter tidligere hendelser eller øvelser.

2.4 METODE OG VURDERING AV DATAGRUNNLAG

Oppdraget er gjennomført i samsvar med standarden for forvaltningsrevisjon (RSK 001). Dette innebærer blant annet at Kommunedirektøren har fått en orientering om oppdraget før oppstart, og en mulighet til å uttale seg om utkast til rapport før endelig rapportering. Kommunedirektørens kommentarer til rapporten, og revisors eventuelle bemerkninger til disse, blir tatt inn avslutningsvis i denne rapporten.

Før rapporten ble sendt til Kommunedirektøren for uttalelse ble rapporten oversendt til FARTT for faktaverifikasjon.

Oppdraget bygger på intervjuer, dokumentgjennomganger, penetrasjonstest og selvstendige analyser.

Hver problemstilling vurderes opp mot de utvalgte revisjonskriteriene. Dette synliggjøres av vurderingskriteriene for revisjonen som er fire nivåer, og er fremstilt i tabellen under.

EVALUERING:
Undersøkte forhold avviker i *svært stor grad* fra revisjonskriteriene.
Undersøkte forhold avviker i *stor grad* fra revisjonskriteriene.
Undersøkte forhold avviker i *noen grad* fra revisjonskriteriene.
Undersøkte forhold *møter i stor grad* revisjonskriteriene.

2.5 AVGRENSNINGER

Forvaltningsrevisjonen har vurdert personvern i relasjon til god informasjonssikkerhet, blant annet ved vurdering av etablerte sikkerhetstiltak, tilgangsstyring og segregering av data. BDO har ikke gjennomført en analyse av FARTT sitt arbeid opp mot personvernlovgivningen utover dette.

Revisjonen har i hovedsak omfattet felles infrastruktur som driftes av IKT Fjellregionen IKS på vegne av kommunene. Revisjonen har ikke omfattet infrastruktur driftet av andre eksterne parter eller av eierkommunene selv.

Forvaltningsrevisjonen, herunder vurderinger og anbefalinger, er basert på samtaler med representanter og gjennomgang av dokumenter som er tilgjengeliggjort av nøkkelressurser og intervjuobjekter. Det vil alltid være en risiko for at relevante forhold som ikke er avdekket gjennom revisjonen kunne ha medført andre vurderinger og konklusjoner. Vårt arbeid er gjennomført innenfor en begrenset ramme og tidsperiode. Omfanget og fullstendigheten av analysene som er gjort må ses i lys av dette. Vi finner det derfor riktig å presisere at vi ikke kan påta oss ansvar for fullstendigheten eller riktigheten i det grunnlagsmaterialet som har vært utgangspunkt for våre vurderinger. Dersom vi har mottatt uriktige eller ufullstendige opplysninger, har vi ikke hatt anledning til å avdekke dette ut over overordnede rimelighetsvurderinger.

2.6 KORT OM FARTT

IKT Fjellregionen IKS er et interkommunalt selskap, eid av Folldal, Alvdal, Rendalen, Tynset og Tolga. Selskapet omtales som FARTT. FARTT drifter IT systemene, nettverkene og kommunikasjonslinjene hos alle eierkommunene.

Selskapet har en selskapsavtale med eierkommunene, denne ble sist revidert 26. juni 2020. I henhold til selskapsavtalen har FARTT følgende ansvarsområder:

- Selskapet skal utvikle og etablere tekniske løsninger, samt drifte systemer for informasjon og kommunikasjonsteknologi i eierkommunene på de områder der dette er kostnadseffektivt.
- Selskapet skal på vegne av eierne være juridisk avtalepart overfor leverandører i den hensikt å oppnå rabatter og storkundefordeler.
- Selskapet skal utvikle kompetanse på bruk av felles applikasjoner, tilby eierne brukerstøtte og tilpasninger til valgte systemer.
- Selskapet skal ha fokus på digitalisering og fremtidige valg av teknologi og systemer som støtte for kommunal tjenesteproduksjon.
- Selskapet skal ved gjennomføring av prosjekter ha fokus på implementering og gevinstrealisering sammen med eierkommunene.

3 PROBLEMSTILLING 1: STYRER SELSKAPET INFORMASJONSSIKKERHETEN PÅ EN TILFREDSSTILLENDE MÅTE?

3.1 REVISJONSKRITERIER

Problemstillingen handler om hvordan FARTT styrer informasjonssikkerheten i sin egen virksomhet. Med utgangspunkt i ISO/IEC 27001 og NSMs grunnprinsipper for IKT-sikkerhet har BDO utarbeidet følgende revisjonskriterier for å svare ut den overnevnte problemstillingen:

- Selskapet har etablert et styringssystem for informasjonssikkerhet.
- Selskapet har definert roller og ansvar knyttet til arbeid med informasjonssikkerhet.
- Selskapet har utarbeidet styrende dokumenter for informasjonssikkerhet.

3.2 OBSERVASJONER MOT REVISJONSKRITERIENE

3.2.1 Styringssystem for informasjonssikkerhet

Et styringssystem legger grunnlaget for en proaktiv og helhetlig tilnærming til informasjonssikkerhet i en virksomhet. FARTT har utarbeidet en *Informasjonssikkerhetspolicy* som gir de overordnede føringene for arbeidet med informasjonssikkerhet i FARTT og eierkommunene. Policyen består av en side med overordnede prinsipper og er i hovedsak rettet mot behandling av person- og helseopplysninger i relasjon til personvernforordningen. Generelle prinsipper for informasjonssikkerhet er i liten grad definert utover dette. Policyen er utarbeidet og godkjent i 2019.

Mer detaljerte beskrivelser av policyer, ansvar og organisering, retningslinjer og rutiner er beskrevet i *IKT-sikkerhetshåndbok for FARTT kommunene*. Dette dokumentet danner grunnlaget for arbeidet med informasjonssikkerhet i FARTT og eierkommunene. I dokumentet er det særskilt definert at sikkerhetshåndboken skal revideres og oppdateres minimum årlig som del av ledelsens gjennomgang. Sikkerhetshåndboken er sist oppdatert i 2015. Gjennom revisjonen er vi opplyst om at dette arbeidet pågår.

FARTT har benyttet Neupart som støtteverktøy for forvaltning av styringssystemet for informasjonssikkerhet til nå, men har planer om å bytte til Compilo i løpet av høsten 2023. FARTT ønsker å bytte til et nytt system på grunn av kompleksiteten i Neupart, og at dette ikke har lagt til rette for å kunne operasjonalisere styringssystemet på en optimal måte.

Gjennom referater fra operativ sikkerhetsgruppe fremgår det at det jobbes kontinuerlig med informasjonssikkerhet gjennom året. Det foreligger referat fra møtene som beskriver aktiviteter og status på ulike tiltak.

3.2.2 Roller og ansvar

FARTT sin organisasjon består av 11 ansatte. Daglig leder er utpekt som overordnet ansvarlig for IKT-sikkerhet i FARTT, men utover dette er det ikke definert en rolle som informasjonssikkerhetsleder (CISO). Hva som inngår i rollen som ansvarlig for IKT-sikkerhet er ikke ytterligere beskrevet.

FARTT har opprettet en operativ sikkerhetsgruppe som består av utvalgte ansatte med interesse og ansvar for informasjonssikkerheten. Den operative sikkerhetsgruppen har som formål å drive frem det løpende arbeidet med informasjonssikkerhet i FARTT. BDO har gjennomgått et utvalg referater

fra møtene til sikkerhetsgruppen i 2023 og dokumentene beskriver status på aktiviteter og ulike tiltak, slik som styringssystem, beredskap og øvelser, risikovurderinger, trusselvurderinger, klientsikkerhet, kurs og kompetanseheving, informasjon til interne og eksterne brukere samt oppfølging av andre tiltak.

FARTT har etablert et IKT-sikkerhetsutvalg som består av en representant fra hver eierkommune og en representant fra FARTT. Utvalget ledes av organisasjonsrådgiver i Rendalen kommune. Formålet til utvalget er å følge opp arbeidet med informasjonssikkerhet i FARTT, samt veilede og være en rådgivende part. Representantene i utvalget har ingen særskilt, faglig eller teknisk kompetanse relatert til informasjonssikkerhet.

Gjennom samtaler med ansatte i FARTT har flere uttalt at de ikke har et særskilt ansvar knyttet til informasjonssikkerhet, ut over det som er en del av deres vanlige arbeidsoppgaver og stillingsinstruks. Driftsleder i FARTT poengterte at han og resten av driftsteamet har ansvar for overvåkning, drift av servere og arbeid med brannmurer, og det som beskrives som teknisk sikkerhet i disse løsningene.

Frem til 2019 hadde hver kommune egne IKT-rådgivere, men dette ble endret og nå er alle IKT-rådgivere ansatt i FARTT. Av samtaler fremkommer det at det har vært lite praktiske endringer knyttet til overføringen, ut over at alle nå kan forholde seg til en felles ledelse. IKT-rådgiverne sitter fortsatt en dag ute hos de enkelte kommunene hver uke.

IKT-rådgiverne har gjennom arbeidet ute i kommunene et større ansvar for klienter og nettverksnoder. Eksempler på arbeidsoppgaver er å bytte ut nettverksnoder eller klienter ved feil eller end-of-life, og å bistå med diverse IT-support for ansatte i kommunen.

3.2.3 Styrende dokumenter

FARTT har utarbeidet en overordnet strategi gjennom *IKT-strategi for IKT Fjellregionen IKS og eierkommunene Folldal, Alvdal, Rendalen, Tolga og Tynset 2017-2020*. Av denne fremkommer det 5 målområder, hvorav å ivareta informasjonssikkerheten er ett av områdene.

Det er utarbeidet et dokument knyttet til ansvarsforhold for informasjonssikkerheten i FARTT og kommunene. Dokumentet spesifiserer hvem som er behandlingsansvarlig og sikkerhetsansvarlig i kommunene. Dokumentet spesifiserer også hvem som er enhetsleder og systemansvarlig for de ulike fagområdene/-systemene i kommunen.

Som beskrevet under 3.2.1 ovenfor er det utarbeidet en IKT-sikkerhetshåndbok for ansatte i kommunene. Denne ble sist revidert 27. mai 2015.

Det er utarbeidet flere policyer, retningslinjer og rutiner for ansatte i kommunene og FARTT, herunder en policy for informasjonssikkerhet, retningslinjer for sosiale medier, internett og epost, beredskapsplan, varslingsrutiner og varslingslister med detaljerte prosedyrer for informasjonsansvarlig og kriseleder, risikovurderinger og tiltaksplan og oversikt over ansvarsforhold IKT-sikkerhet. Flere av de styrende dokumentene er utarbeidet i 2022 og 2023. I løpet av våren 2023 har det spesielt vært fokus på å etablere gode rutiner for beredskap og varsling.

3.3 REVISORS VURDERING

Et styringssystem for informasjonssikkerhet må utarbeides med bakgrunn i en virksomhets størrelse og funksjon. Det foreligger en struktur med overordnede policyer, en detaljert IKT-sikkerhetshåndbok og retningslinjer og rutiner for informasjonssikkerhet i FARTT. Til sammen vurderes disse å utgjøre grunnlaget for et styringssystem for informasjonssikkerhet. Vi vurderer imidlertid at operasjonaliseringen av styringssystemet kan forbedres gjennom prosesser for gjennomføring av ledelsens gjennomgang, internrevisjoner, tydeliggjøring og forankring av roller

og ansvar knyttet opp mot styringssystemet for informasjonssikkerhet, og det å skape en rød tråd mellom risikovurderinger, prioritering av aktiviteter og utførelsen av disse. Vi vurderer også at manglende oppdatering av de øverste dokumentene, *Informasjonssikkerhetspolicy* og *IKT-sikkerhetshåndboken*, indikerer at disse ikke brukes som retningsgivende i det daglige arbeidet med informasjonssikkerhet.

Det øverste ansvaret for informasjonssikkerhet ligger hos daglig leder, men BDO har ikke identifisert noen i FARTT som har rollen som informasjonssikkerhetsleder. Det er heller ikke definert hva en slik rolle skal omfatte. Den operative sikkerhetsgruppen har en viktig funksjon, og virker å være en pådriver for at arbeidet med informasjonssikkerhet følges opp gjennom planer og aktiviteter, og har kontinuerlig fokus på forbedringstiltak og fremdrift. BDO vurderer at ansvaret for informasjonssikkerhet bør tydeliggjøres, beskrives og plasseres i organisasjonen.

Sikkerhetsutvalget vurderes også å ha en viktig funksjon, både som bindeledd mellom FARTT og kommunene, men også for å påse at sikkerhetstiltak fungerer etter hensikt ute i kommunene. BDO vurderer at utvalget med fordel kunne styrket den faglige kompetansen relatert til informasjonssikkerhet for å fungere som en rådgivende funksjon.

3.4 KONKLUSJON

Revisor vurderer at de undersøkte forholdene *avviker i noen grad* fra revisjonskriteriene. Det eksisterer et styringssystem for informasjonssikkerhet, og revisor vurderer at dette etterleves og er operasjonalisert i selskapet. Det er imidlertid et forbedringspotensial knyttet til definering av roller og ansvar knyttet til informasjonssikkerhetsarbeidet, og oppdatering av styrende dokumenter.

3.4.1 Anbefalte tiltak

BDO anbefaler følgende tiltak, i en ikke-prioritert rekkefølge:

- Oppdatere Informasjonssikkerhetspolicy og IKT-sikkerhetshåndbok tilpasset organisasjon, trusselbilde og sikkerhetsbehov for 2023. Gjennomgang og oppdatering av disse dokumentene bør inngå som en del av en ledelsens gjennomgang, og utføres minimum årlig.
- Supplere sikkerhetsutvalget med mer kompetanse på informasjonssikkerhet, f.eks. knytte til seg en ekstern rådgivende part.
- Tydeliggjøre, beskrive og plassere det overordnede ansvaret for informasjonssikkerhet i FARTT.

4 PROBLEMSTILLING 2: BLIR SIKKERHETSRISIKOER IDENTIFISERT OG HÅNDTERT?

4.1 REVISJONSKRITERIER

Med utgangspunkt i standarden ISO/IEC 27001 og NSMs grunnprinsipper for IKT-sikkerhet har BDO utarbeidet følgende revisjonskriterier for å svare ut den overnevnte problemstillingen:

- Selskapet har kartlagt alle enheter og programvare som er i bruk
- Selskapet har kontroll på alle identiteter og tilganger
- Selskapet har utarbeidet, og reviderer jevnlig, risiko- og sårbarhetsanalyse av IKT-systemene.

4.2 Observasjoner mot revisjonskriteriene

4.2.1 Kartlegging av enheter og programvare

FARTT startet i 2023 migrering og innrullering av klienter, herunder PC-er og mobiltelefoner, til forvaltningssystemet Microsoft Intune. I samtaler med BDO har FARTT informert om at det har vært god progresjon på innrulleringen og at det innen utgangen av mai 2023 kun var enkelte enheter hos Tolga kommune som ikke var innrullert i Intune. Disse enhetene er eldre klienter som ikke støttes av Microsoft Intune.

FARTT informerte i samtale med BDO at de kontrollerer hvilken programvare som kan installeres på PC-ene til ansatte i kommunen med verktøyet Microsoft Configuration Manager. FARTT har videre anledning til å tvinge gjennom oppdateringer av programvarer og operativsystem for å sikre at kjente sårbarheter fjernes. I penetrasjonstesten til BDO ble det avdekket at det var mulig å kjøre tredjepartsprogrammer og script fra en ekstern USB minnepenn hvis man er innlogget med aktiv brukerkonto på en klient.

BDO er informert om at det ikke er lokal administratorrettighet på klienter innrullert i Intune, og FARTT bekrefter at det er kun global admin som kan elevere kontoer og gi mer rettigheter på egen bruker.

BDO er oversendt en oversikt over serverne til FARTT som viser at operativsystemet på enkelte av serverne nærmer seg «end of support». Gjennom samtaler ble det bekreftet at det er en pågående utfasing av gamle operativsystemer og at dette vil være ferdigstilt før dato for «end of support» inntreffer. I penetrasjonstesten til BDO oppdaget vi en eldre SQL-server på Tynset sitt kommunenett. Denne serveren har BDO ikke funnet i den oversendte oversikten over servere.

FARTT har oversikt over alle Chromebook-klienter i forvaltningssystemet G-Suite. Gjennom samtaler fremkom det at FARTT ikke har gjort vurderinger av om de bør benytte seg av spesifikk herding av enhetene ut over standardinnstillingene.

4.2.2 Kontroll på identiteter og tilganger

FARTT bruker Active Directory (AD) og Azure Active Directory (Azure AD) til å styre brukerkontoer og tilganger til systemer og infrastruktur. For at en ansatt skal få tilgang til FARTT sin AD, må en leder sende inn et autorisasjonsskjema hvor det skal fremgå hva den ansatte skal ha tilgang til, samt hvilke fagsystemer personen eventuelt trenger. FARTT er ikke ansvarlig for å gi tilganger i

fagsystemene, da dette ivaretas av eierkommunene. På revisjonstidspunktet hadde FARTT 2813 unike brukerkontoer i Azure AD, hvorav 286 av disse var gjestebrukere.

Ved avslutning av arbeidshold skal nærmeste leder sende inn sluttskjema til FARTT. I sluttskjemaet skal det fremkomme når personen har siste arbeidsdag. FARTT vil manuelt registrere sluttdato, slik at personen mister tilgang ved endt arbeidsforhold. FARTT er kjent med at sluttskjema ikke alltid sendes inn, og har koblet AD opp mot lønns- og personalsystemet til kommunene. Hver natt kjøres det en automatisk synkronisering mellom AD og lønns- og personalsystemet for å kontrollere at det kun er faktiske ansatte som til enhver tid har aktive AD-brukere.

Som nevnt ovenfor er det 286 gjestebrukere i FARTT sin Azure AD. I samtaler forklarte FARTT at dette kan være eksterne personer som er invitert inn i Teamsrom, eller som er gitt tilgang til spesifikke SharePoint-områder. Ved gjennomgang av sikkerhetskonfigureringene til FARTT sin Microsoft 365 ble det identifisert avvik fra anbefalte beste praksis, blant annet ved at alle brukere kan invitere inn gjestebrukere uten godkjenning av administrator og at det ikke er satt en regel for hvor ofte en gjestebruker må fornyes, eller om de deaktiveres etter et gitt antall inaktive dager.

Når det kommer til tilgang til de ulike fagsystemene i kommunene er det de enkelte kommunene selv som er ansvarlig for tildeling av tilganger og rettigheter. De fleste fagsystemene har en kobling mot AD for å autentisere brukeren, men det er enkelte unntak. Ett unntak er systemet for vann- og avløp.

Fagsystemer tilgjengeliggjøres for ansatte ved at nærmeste leder oppgir hvilke fagsystemer den ansatte trenger tilgang til i autorisasjonsskjemaet. Dette skjemaet fylles ut ved ansettelse og oversendes til FARTT. Hvis det oppstår behov for tilgang til andre fagsystemer, skal et nytt autorisasjonsskjema sendes inn. En ansatt må både få systemet tilgjengeliggjort av FARTT på sin klient og deretter få tilgang til systemet av systemansvarlig i kommunen via AD.

Det er kommunene som selv er ansvarlig for å gjennomgå tilganger og rettigheter i fagsystemene via sine systemansvarlige.

Ansatte i FARTT har Global Admin-rettigheter i Azure AD. For en av disse kontoene var conditional access deaktivert. Denne brukerkontoen var knyttet til en enkelt person, og var ikke en «break the glass» konto. Hvis det hadde vært en «break the glass» konto kunne dette forklart hvorfor den var unntatt conditional access. Av samtaler fremgikk det at det ikke gjøres vurderinger knyttet til hvilke tilganger hver enkelt ansatt i FARTT har behov for, men at det kun er gjort en generell vurdering av at ansatte trenger vide rettigheter for å utføre sine arbeidsoppgaver på tvers av kommunene.

4.2.3 Risiko- og sårbarhetsanalyse av IKT-systemene

BDO er oversendt en Risiko- og sårbarhetsanalyse (ROS-analysen) for FARTT som ble gjennomført 22. mars 2023.

Risikoskjemaet bygger på risikobeskrivelse, eksisterende risikoreduserende tiltak, begrunnelse for konsekvensvurdering og begrunnelse for vurdering av tilhørende sannsynlighet. Alle risikoer er tildelt en konsekvens og sannsynlighet, men av 57 risikoer har kun 31 fått begrunnelse for vurdering av konsekvens og kun 8 har fått begrunnelse for vurdering av sannsynlighet.

I risikoskjemaet er det også en tiltaksplan som FARTT hadde oppfølging av den 29. mars 2023. Alle risikoer har fått tildelt et tiltak eller en beskrivelse i tiltaksplanen. Av 57 risikoer har ingen blitt tildelt en risikoeier, frist for igangsettelse eller planlagt sluttdato.

Av de 57 risikoene valgte FARTT å ikke akseptere to av risikoene. Av tiltaksplanen fremgår det at de to risikoene i etterkant er akseptert, uten at risikoen er redusert, eller at tiltakene er registrert som gjennomført.

BDO er informert om at kommunene og FARTT har et to-delt ansvar for risikoanalyser knyttet til de ulike systemene FARTT drifter. BDO er ikke oversendt noen av disse og har derav ikke vurdert analysenes kvalitet.

4.3 REVISORS VURDERING

FARTT er nesten ferdig med å innrullere alle klienter i Intune. Dette er et viktig steg for å kunne identifisere og håndtere sikkerhetsrisikoer. BDO har ikke hatt tilgang til og vurdert selve oppsettet i Software Center, men BDOs penetrasjonstest avdekket muligheten til å kjøre script og annen programvare ut over standardpakken, noe som indikerer behov for sterkere herding av klientene.

Den daglige kontrollen mellom lønns- og personalsystemet opp mot AD sikrer at tidligere ansatte mister tilgangene fra sluttdato selv om en leder glemmer å informere FARTT om oppsigelsen. Fagsystemer som ikke er knyttet opp mot AD faller utenfor denne sikkerhetskontrollen og kan innebære en høyere risiko med hensyn til at brukerkontoer ikke automatisk blir deaktivert når ansatte slutter.

FARTT benytter seg ikke av beste praksis knyttet til gjestebrukere i Azure AD. Med dagens løsning risikerer FARTT at de ikke har kontroll over antall gjestebrukere, ettersom alle kan invitere gjestebrukere og at disse ikke automatisk deaktiveres eller slettes etter et gitt tidsintervall.

Det er videre identifisert et avvik fra beste praksis knyttet til den generelle bruken av global admin rettigheter blant FARTT sine ansatte. Beste praksis er å begrense bruken av global admin til et absolutt minimumsnivå, og heller bruke mer granulære rettigheter for andre administratorbehov. Prinsippene for minste privilegium bør til enhver tid følges, spesielt for høyt privilegerte rettigheter.

FARTT har gjennomført en risikovurdering i 2023, men BDO anser denne som mangelfull. BDO savner dokumentasjon av hvilke vurderinger som er gjort av FARTT. BDO vurderer det videre som kritisk at tiltak og risikoer ikke tildeles en eier for videre oppfølging. Arbeid med risiko er en kontinuerlig prosess og uten god dokumentasjon og ansvarliggjøring av enkelte for videre oppfølging vil prosessen kunne stagnere.

BDO vurderer derfor at FARTT ikke har gjennomført en risikovurdering med tilfredsstillende kvalitet. Dette kan få konsekvenser for det videre sikkerhetsarbeidet til FARTT. En virksomhet bør velge sin sikkerhetsstrategi og tiltak med bakgrunn i det risikobildet og de risikovurderingene de har gjennomført.

BDO stiller også spørsmål ved at oppfølgingen av tiltaksplanen inntraff kun syv dager etter gjennomført risikovurdering. For BDO fremstår dette kun som en avsjekk for at det er gjort på papiret, og ikke at tiltaksplanen faktisk er fulgt opp i praksis. Dette underbygges av at det ikke er bekreftet hvorvidt tiltak er gjennomført og at FARTT aksepterer samme risiko som man syv dager tidligere ikke aksepterte.

4.4 KONKLUSJON

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

4.4.1 Anbefalte tiltak

BDO anbefaler følgende tiltak, i en ikke-prioritert rekkefølge:

- Fullføre innrulleringen av forvaltningssystemet og etablere prosesser for kontinuerlig vedlikehold.
- Begrense bruken av global admin-rettigheter til absolutt minimumsnivå, og heller bruke mer granulære rettigheter for andre administratorbehov.
- Etablere rutiner for sikkerhetskonfigurering i Microsoft 365 i henhold til beste praksis, inkludert forvaltning av gjestebrukere.
- Heve kvaliteten i risiko- og sårbarhetsvurderinger som gjennomføres, herunder dokumentasjon av vurderinger og metodisk oppfølging av identifiserte risikoer og tiltak.

5 PROBLEMSTILLING 3: BLIR INFORMASJON OG INFORMASJONSSYSTEMER BESKYTTET IHT. BESTE PRAKSIS?

5.1 REVISJONSKRITERIER

Med utgangspunkt i ISO/IEC 27001 og NSMs grunnprinsipper for IKT-sikkerhet har BDO utarbeidet følgende revisjonskriterier for å svare ut den overnevnte problemstillingen:

- Selskapet har etablert et regime for sikker IKT-arkitektur og konfigurasjon.
- Selskapet har oversikt og kontroll over hele livsløpet til de tjenestene som forvaltes på vegne av kommunen og som er tjenesteutsatt.
- Selskapet har en plan for regelmessig sikkerhetskopiering av all virksomhetsdata for kommunene

5.2 Observasjoner mot revisjonskriteriene

5.2.1 Etablert regime for sikker IKT-arkitektur og konfigurasjon

FARTT leier plass til hosting av servere i datahallen til leverandøren Duett, lokalisert på Tynset. Samtlige servere er lokalisert i samme datahall og FARTT har ingen sekundær lokasjon for hosting. I samtaler har FARTT påpekt at dersom det skjer en større uønsket hendelse i datahallen til Duett (vann/brann/terror ol.) vil det sannsynligvis ta lang tid å få satt opp driftsmiljøet til FARTT på en alternativ lokasjon.

FARTT eier og vedlikeholder selv de fysiske serverne i datahallen og har i tillegg ansvaret selv for å sikre internett til serverne. Duett har ansvaret for sikring av fysisk tilgang til senteret, sikring mot brann og vannskader og redundant strømtilførsel. Datahallen til Duett har sikringstiltak mot brann og vann i henhold til den internasjonale standarden EN-1047-2. I følge FARTT er det et begrenset antall ansatte som har tilgang til serverrommet, og tilgang til datarommet reguleres med både nøkkelkort og fysisk nøkkel.

FARTT har avtale med kun en ISP ("internet service provider") for leveranse av internett. FARTT har informert BDO om at de tidligere har forsøkt å få på plass avtale med en ISP til for å styrke redundansen, men at dette har vist seg vanskelig å få til grunnet begrenset kapasitet på linjenettet i regionen.

For autentisering og styring av rettigheter inn mot IKT-infrastruktur og systemer bruker FARTT en on-prem Active Directory (AD) som har Azure AD Connect sync, som synkroniserer AD med alle brukerkontoer i FARTT sin Azure AD tenant. Dette betyr at FARTT administrerer alle brukerkontoer og tilganger for alle kommuner i samme AD-tenant. I samtale med daglig leder i FARTT ble det informert om at FARTT tidligere har hatt samtaler med Atea knyttet til hvorvidt det burde settes opp en AD-tenant for hver enkelt kommune, eller om løsningen med en felles AD for alle kommunene skal videreføres.

Som nevnt tidligere i rapporten tilgjengeliggjør FARTT programvare og fagsystemer for de ansatte i kommunene. For å sikre separasjon av data på tvers av kommunenes fagsystemer har FARTT egne versjoner av fagsystemene for hver enkelt kommune. For de tjenestene hvor flere kommuner samarbeider er det felles fagsystem.

Ved innlogging utenfor regulerte on-prem lokasjoner kreves det bruk av MFA (multifaktor autentisering) som aktiveres via conditional access policyer i Azure AD. Metoder som er godkjent

for multifaktor er enten Microsoft Authenticator eller SMS. BDO har ikke fått tilsendt passordpolicy for FARTT. I samtaler med FARTT er det informert om at det er krav om 14 tegn, men ikke krav om spesielle tegn. Det var tidligere krav om jevnlig utskiftning av passord, men dette kravet gjelder ikke lenger.

FARTT bruker Intune til å sette opp og administrere alle Windows-klienter som brukes i kommunene. FARTT har ikke kunnet vise til at det brukes noen herdeprofil (som Windows Security Baseline eller CIS Benchmark) som utgangspunkt for å sikre beste praksis for sikkerhetsinnstillinger når maskinene settes opp. For Windows-servere brukes det heller ikke noen herdeprofil som utgangspunkt. Servere settes opp manuelt og FARTT kunne ikke vise til noen skriftlig konfigurasjonsmal. FARTT har startet planlegging og testing av innrullering av mobiltelefoner i Intune, og det ble ikke identifisert noen herdeprofil for mobiltelefoner heller.

5.2.2 Oversikt og kontroll over hele livsløpet til tjenester som er tjenesteutsatt

I anbudsprosesser har FARTT angitt kvalifikasjonskrav og avvisningsregler for leverandører. Disse danner grunnlag for FARTT sine avtaler med leverandørene. Under intervjuer har FARTT forklart at det ikke gjennomføres sikkerhetsrevisjoner av leverandørene. FARTT forklarte at de har tillit til at leverandørene leverer det som loves.

BDO er oversendt en oversikt over databehandleravtaler. Av oversikten fremgår det at det er inngått databehandleravtaler med alle leverandører på listen, men i samtaler med BDO påpekte FARTT at det fortsatt mangler databehandleravtaler med enkelte leverandører.

5.2.3 Plan for regelmessig sikkerhetskopiering av all virksomhetsdata

FARTT bruker systemet Veeam Software til å ta sikkerhetskopier av alle servere som hostes hos Duett. FARTT tar ikke selv sikkerhetskopiering av data lagret i skyen. Veeam Software er del av FARTT sitt AD-domene og lagrer en backup i Duett sin datahall, samt en kopi via Veeam i rådhuset på Tynset. I tillegg lagres en tredje backup i Duett sin datahall, men separert fra FARTT sitt AD-domene. I følge FARTT er denne tredje backupen immutable og kan ikke redigeres eller slettes før det er gått 180 dager. Det tas ikke backup til tape.

Det er ikke gjennomført noen øvelser som tester full gjenoppretting fra backup og det ble ikke gitt noen informasjon fra FARTT som tilsier at øving på gjenoppretting og disaster recovery er noe som har høy prioritet. FARTT har ingen separat lokasjon med hele eller deler av infrastrukturen stående klar, i tilfelle det må gjøres gjenoppretting fra backup grunnet problemer med Duett sitt datasenter eller et pågående cyberangrep.

5.3 REVISORS VURDERING

BDO vurderer det til at FARTT har flere betydelige svakheter i sin IKT-arkitektur og prosedyre for sikker konfigurering, sammenlignet med anbefalte beste praksis og i forhold til hva andre norske driftsleverandører har av sikringstiltak.

FARTT har ikke et sekundært datasenter som tjenestene kan gjøre fail-over til og driftes fra hvis datasenteret til Duett får problemer, og heller ikke en disaster recovery site stående klar hvis produksjonsmiljøet må gjenopprettes etter en alvorlig hendelse på datasenteret. Dette gjør kommunene svært avhengige av at Duett sitt datasenter til enhver tid er tilgjengelig og ikke blir rammet av en større negativ hendelse eller feil. I tillegg har FARTT kun avtale med en ISP, slik at ved feil hos internett-leverandøren vil FARTT, eierkommuner og lokasjoner kunne miste tilgangen til de fleste tjenester.

FARTT forvalter brukerkontoer for alle eierkommunene i en og samme Azure AD tenant. Dette åpner opp muligheten for at en sofistikert angriper kan bevege seg horisontalt mellom kommunene

sine systemer i en situasjon hvor angriper kompromitterer en høyt privilegert konto. Dette gjør det ekstra viktig at FARTT har god kontroll på tilganger og brukerkontoer. Som beskrevet tidligere i rapporten har ansatte i FARTT globale admin-rettigheter. Manglende krav om passordkompleksitet og ingen tvungen rotasjon av passord er også avvik fra anbefalte beste praksis.

I tillegg bruker FARTT hverken herdeprofiler for PCer, servere eller mobiltelefoner. Herdeprofiler basert på CIS Benchmarks eller Windows Security Baseline inneholder flere hundre sikkerhetskonfigureringer som er stilt i henhold til anbefalte beste praksis. Dette gjør kommunenes servere og klienter unødvendig sårbare.

BDO har fått informasjon om at det ikke foreligger databehandleravtaler, eller oppdaterte databehandleravtaler i samsvar med de tjenestene som leveres, med alle underleverandører til FARTT. Dette innebærer risiko for manglende etterlevelse av personvernforordningen.

Manglende rutiner for regelmessig test av full gjenoppretting fra backup, eller gjenoppretting fra backup på alternativ lokasjon, medfører risiko for uakseptable lang nedetid etter en eventuell hendelse.

5.4 KONKLUSJON

Revisor vurderer at de undersøkte forhold *avviker i stor grad* fra revisjonskriteriene. Det er avdekket flere betydelige svakheter i IKT-arkitektur og konfigurering. Selskapet gjør heller ingen sikkerhetsrevisjoner av underleverandører eller test av gjenoppretting og disaster recovery.

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

5.4.1 Anbefalte tiltak

BDO anbefaler følgende tiltak, i en ikke-prioritert rekkefølge:

- Innføre tiltak for å redusere konsekvensene ved hendelser mot datasenteret, eksempelvis en redundant løsning i sky eller en sekundær lokasjon. Vi anbefaler samtidig for å undersøke mulighetene for alternative ISP-løsninger.
- Innføre rutiner for test av gjenoppretting fra backup og disaster recovery øvelser for gjenoppretting på alternativ lokasjon. Dette bør i første omgang omfatte de mest kritiske systemene i kommunene.
- Gjennomføre og dokumentere en risikovurdering knyttet til bruken av en felles Azure AD tenant for alle kommunene i FARTT. Innføre tiltak som sikrer seperasjon mellom de ulike kommunene.
- Gjennomgå sikkerhetskonfigureringene i Microsoft 365 og Azure AD og oppdatere disse i henhold til beste praksis.
- Innføre standard herdeprofiler basert på beste praksis for PCer, servere og mobiltelefoner.
- Etablere rutiner for sikkerhetsrevisjoner basert på kritikalitet og risiko.
- Påse at det er løpende føres oversikt over alle underleverandører, og at avtaler og databehandleravtaler med underleverandørene reflekterer kommunenes sikkerhetskrav og de tjenestene som leveres.

6 PROBLEMSTILLING 4: HVORDAN OPPDAGES AVVIK OG MULIGE TRUSLER MOT VIRKSOMHETEN?

6.1 REVISJONSKRITERIER

Med utgangspunkt i ISO/IEC 27001 og NSMs grunnprinsipper for IKT-sikkerhet har BDO utarbeidet revisjonskriterier som svarer ut den overnevnte problemstillingen:

- Selskapet har etablert sikkerhetsovervåkning av utvalgte deler av IKT-systemet.
- Selskapet har rutiner for å oppdage og fjerne kjente sårbarheter og trusler.
- Selskapet har gjennomført inntrengningstester på utvalgte IKT-systemer.

6.2 Observasjoner mot revisjonskriteriene

6.2.1 Etablert sikkerhetsovervåkning av utvalgte IKT-system

FARTT bruker et system for driftsmonitorering og vedlikehold av servere og nettverksutstyr. Systemet overvåker verdier som blant annet responstid, temperatur og lagringskapasitet, og flagger eventuelle avvik og feil. FARTT bruker et system for sikkerhetsmonitorering av servere, klienter og brukerkontoer. Systemet henter inn data løpende og analyserer informasjonen for å finne mistenkelig aktivitet som virus eller en kompromittert klient.

Både systemet for driftsmonitorering og systemet for sikkerhetsmonitorering har automatisert monitorering, og ved kritiske hendelser og avvik sender systemene ut varsler til ansatte i FARTT. Ansatte i FARTT følger opp varsler fra systemene fra kl. 07:00 – 15:30 i ukedager, men ut over disse tidspunktene er ingen i FARTT som er pålagt å følge opp varsler fra systemene. FARTT har informert om at de er forpliktet til å ivareta operativ drift, men har ikke operativ beredskap ut over de overnevnte tidspunktene. FARTT har ingen avtale med systemleverandørene, eller annen tredjepart, for monitorering og hendelseshåndtering når ansatte i FARTT ikke er på jobb. FARTT har heller ingen generell avtale med en samarbeidspartner innen cybersecurity, slik at alt av varsler og hendelser blir håndtert av FARTT på egenhånd. FARTT har i dag ikke noen ansatte med dedikert, tung kompetanse på cybersikkerhet, men er i tett dialog med samarbeidspartnere.

All e-post som mottas hos kontoer med tilknytning til FARTT går først gjennom et e-post filter satt opp av en ekstern leverandør. Filteret inkluderer blant annet antispam-, anti-phishing- og antivirusteknologi for å hindre ondsinnede e-poster. E-poster som kommer gjennom filteret blir så vurdert av Exchange Online, før et sikkerhetsmonitoreringssystemet gjør vurderinger når e-posten åpnes på klienten.

FARTT overvåker brukerkontoer gjennom Azure AD Identity Protection og sikkerhetsmonitoreringssystemet. Det er konfigurert flere triggere som vil definere en brukerkonto som risikoutsatt, blant annet basert på brukerkontoens IP-historikk, pålogging fra land og regioner som er sett på som høyrisikoland og ved flere mislykkede påloggingsforsøk. Hvis en brukerkontos risikoklassifiseres som høy vil dette flagges i sikkerhetsmonitoreringssystemet og en ansatt i FARTT får i oppgave å følge opp kontoen. Brukere som får klassifisert risikoen som høy blir ikke automatisk deaktivert av Identity Protection, men krever manuell oppfølging av FARTT.

6.2.2 Rutiner for å oppdage og fjerne kjente sårbarheter og trusler

FARTT gjennomfører periodisk vedlikehold med oppdatering av servere. Dersom det kommer ut kritiske oppdateringer i mellomtiden, så kjøres disse oppdateringene fortløpende.

Når sårbarheter eller trusler oppdages så skal disse registreres i systemet Compilo, der ansvaret for å følge opp saken tildeles en ansatt i FARTT. BDO har ikke vurdert den faktiske oppfølgingen av avvik registrert i Compilo, men har observert at større avvik og sårbarheter følges opp i den operasjonelle sikkerhetsgruppen.

I samtaler med BDO informerte FARTT om at ansatte følger med på utviklingen i sårbarhets- og trusselbildet via kilder som NSM, PST, Kommune-CSIRT og HelseCERT. Dog, det er ikke identifisert noen tydelig systematikk og rollefordeling i forhold til denne oppfølgingen.

6.2.3 Gjennomført inntrengingstester på utvalgte IKT-systemer

FARTT har ikke tidligere gjennomført inntrengningstester mot sine IKT-systemer. BDO gjennomførte våren 2023 en tredelt test med utsidetest, innsidetest og klienttest. Testene identifiserte flere betydelige sårbarheter, blant annet inneholder kommunenettverket i Tynset flere sårbare maskiner, og flere switcher i nettverket har åpen pålogging uten passord. Disse sårbarhetene har sannsynligvis eksistert over lengre tid.

HelseCERT og Kommune-CSIRT gjennomfører jevnlig sårbarhetsscanning av FARTT og kommunenes domener og ytre porter. Resultatene fra disse scannene og fra BDO sin ytre test viser at det er få sårbarheter for en angriper å ta utgangspunkt i fra utsiden.

6.3 REVISORS VURDERING

BDO vurderer at FARTT har gode systemer for å identifisere og varsle om sårbarheter på servere, klienter og e-post. Systemene som FARTT benytter er alle viktige moderne og gode løsninger. I tillegg har FARTT god monitorering av eksponerte IP-adresser og offentlige domener via jevnlige sårbarhetsscanninger levert av HelseCERT og Kommune-CSIRT.

BDO stiller derimot spørsmål ved manglende oppfølging av varsler fra monitoreringssystemene 24/7, enten fra ansatte i FARTT eller via avtale med en ekstern leverandør av SOC-tjeneste (Security Operations Center). Dagens situasjon skaper usikkerhet i forhold til om, og hvem, hos FARTT som eventuelt følger opp varsler utenfor normal arbeidstid, noe BDO ser på som et betydelig avvik.

I tillegg har ingen i FARTT tung kompetanse innen cybersikkerhet, noe som vil være en svakhet både i forhold til evaluering av varsler, utarbeidelse av tiltak for håndtering av varsler og håndtering av en faktisk cyberhendelse.

FARTT har heller ingen historikk for å gjennomføre penetrasjonstester, hverken fra utside eller innside. BDOs test fant flere betydelige sårbarheter som sannsynligvis har vært der over lengre tid. BDOs test har vært både tidsbegrenset og hatt et begrenset omfang, slik at det ikke er urimelig å anta at det fortsatt eksisterer ukjente sårbarheter i FARTT sin infrastruktur. Beste praksis er å utføre jevnlig penetrasjonstesting, minimum årlig, der omfang justeres basert på en kritikalitetsvurdering av systemer og infrastruktur, samt endringer i trusselbildet.

6.4 KONKLUSJON

Revisor vurderer at de undersøkte forhold *avviker i noen grad* fra revisjonskriteriene. Det er etablert rutiner for sikkerhetsovervåkning og sårbarhetsscanning, men disse omfatter ikke oppfølging av varsler utenfor normal arbeidstid. Videre vurderer vi at FARTT ikke har spesifikk kompetanse for å vurdere og håndtere cyberhendelser på en forsvarlig måte. Det er ikke tidligere gjennomført inntrengingstester.

6.4.1 Anbefalte tiltak

- Implementere en vaktordning som sikrer at varsler fra sikkerhetsovervåkningen håndteres også utenfor normal arbeidstid.
- Tilknytte seg en leverandør med spesifikk kompetanse innen cybersikkerhet som kan bistå med vurdering og håndtering av varsler og/eller cyberhendelser.
- Etablere rutiner for inntrengingstester basert på kritikalitet og risiko. Denne bør sees i sammenheng med anbefalte tiltak vedrørende sikkerhetsrevisjoner i kapittel 5.4.1.

7 PROBLEMSTILLING 5: BLIR HENDELSER HÅNDTERT PÅ EN TILFREDSSTILLENDE MÅTE

7.1 REVISJONSKRITERIER

Med utgangspunkt i standarden ISO/IEC 27001 og NSMs grunnprinsipper for IKT-sikkerhet har BDO utarbeidet revisjonskriterier som svarer ut den overnevnte problemstillingen:

- Selskapet har et planverk for hendelseshåndtering og som revideres jevnlig.
- Selskapet har gjennomført regelmessige øvelser på informasjonssikkerhetshendelser.
- Selskapet har evaluert og implementert tiltak etter tidligere hendelser eller øvelser.

7.2 OBSERVASJONER MOT REVISJONSKRITERIENE

7.2.1 Planverk for hendelseshåndtering

NSMs grunnprinsipper for IKT-sikkerhet har flere anbefalinger knyttet til hva en beredskapsplan bør inneholde: (1) Krav til gjenopprettelse av IKT-systemer basert på en analyse av konsekvenser for virksomheten, (2) Rolle- og ansvarsbeskrivelse for relevant personell, (3) Krav til opplæring for relevant personell, (4) Klassifiseringsregime for hendelser og grenseverdier for å aktivere krisestab og (5) Krav til testing og øving av planverk og personell.

Styret i FARTT godkjente ny IKT beredskapsplan i februar 2023. I beredskapsplanen har FARTT utarbeidet en oversikt over prioriterte systemer knyttet til lengre nedetid. FARTT har ikke selv gjort en analyse av konsekvenser ved nedetid, men har basert seg på prioriteringene til kommuneledelsen.

Beredskapsplanen har en oversikt over roller og ansvar, beskrivelse, samt vedlegg med mer utfyllende rollebeskrivelser.

Det fremgår ikke av beredskapsplanen, eller annet planverk i FARTT, om det er krav til opplæring i planverket for relevant personell.

Av beredskapsplanen fremgår det at det skal utarbeides handlingsplaner for når ulike hendelser inntreffer. BDO har ikke fått tilsendt handlingsplanene og kan dermed ikke verifisere at de er hensiktsmessig utformet.

7.2.2 Gjennomføring av øvelser på informasjonssikkerhetshendelser

Siden 2019 har FARTT gjennomført 3 øvelser. Gjennom samtaler er det forklart at FARTT har mål om å gjennomføre 2 øvelser i året, men at dette ble vanskelig å gjøre under pandemien. BDO er oversendt evaluering fra flere øvelser.

Evalueringene inneholder en oppsummering av øvelsen, læringspunkter og tiltak for forbedring.

Av evalueringene fremkommer det at de siste 4 øvelsene som er gjennomført i FARTT har vært diskusjonsøvelser. Alle øvelsene er planlagt og gjennomført av egne ansatte i FARTT. Scenarioene for øvelsene har vært ransomware-angrep mot mobiltelefoner, cyberangrep der alle ekomtjenester blir borte, brann i datahall og manglende tilgjengelighet til utvalgte applikasjoner.

I samtaler med daglig leder og leder for sikkerhetsutvalget fremkom det at det er et ønske om å gjennomføre en større beredskapsøvelse, hvor man involverer flere av kommunene, og/eller fylkeskommunen.

7.2.3 Evaluering og implementering av tiltak etter tidligere hendelser eller øvelser

FARTT hadde en større uønsket hendelse 1. november 2022. FARTT etablerte krisestab 2. november og problemet ble løst 8. november 2022.

BDO er oversendt evalueringene som ble gjort i etterkant av hendelse. FARTT har evaluert hva som fungerte, hva som ikke fungerte, og sett på hvilke tiltak som må gjennomføres for å håndtere en tilsvarende situasjon bedre ved neste hendelse. I evalueringen ble det blant annet trukket frem at ressursallokering under en hendelse bør forbedres for å redusere arbeidsbelastningen på nøkkelressurser. I tillegg hadde ikke FARTT fysiske arbeidslokaler som var tilrettelagt for at flere ansatte kunne jobbe effektivt sammen for å løse krisen.

I samtaler med BDO har flere fra FARTT erkjent at de brukte for lang tid på å løse hendelsen.

BDO har fått tilsendt evalueringene fra øvelsene som er gjennomført i 2017, 2018, 2020 og 2023. Alle øvelsene er i etterkant evaluert basert på øvelsens omfang, scenario, og tiltak til forbedring.

BDO har observert at flere av tiltakene som er anbefalt etter tidligere øvelser er blitt fulgt opp av FARTT. Det har blitt utarbeidet en ny beredskapsplan og det har blitt inkorporert en ny rolle i kriseledelsen etter hendelsen i 2022. Etter øvelsen i 2023 var ett av tiltakene at sikkerheten til ansattes mobiltelefoner måtte styrkes. FARTT har i etterkant startet en pilot for å teste innrullering av mobiltelefoner i Intune. Dette vil gi et bedre utgangspunkt for å styrke sikkerheten til mobiltelefoner.

Som beskrevet tidligere i rapporten, har ikke FARTT gjennomført full teknisk gjenoppretting fra backup og heller ikke gjennomført tekniske disaster recovery øvelser. Det er heller ingen konkrete planer om å øve på dette i fremtiden.

7.3 REVISORS VURDERING

BDO vurderer at hendelsen høsten 2022 viser at FARTT ikke håndterte denne på en tilfredsstillende måte og ikke er godt nok forberedt på større uønskede hendelser. Det tok uforholdsmessig lang tid å etablere krisestab og det tok lang tid å løse problemet. Det var også flere organisatoriske prosesser som er viktige i håndteringen av en hendelse som FARTT ikke var godt nok rustet for.

I etterkant av hendelsen, og i etterkant av tidligere utførte øvelser, fremkommer det at FARTT følger opp læringspunkter og anbefalte tiltak. Blant annet oppdaterte FARTT sin beredskapsplan i etterkant av hendelsen. BDO vurderer det som positivt at FARTT gjennomfører evalueringer i etterkant av øvelser og hendelser, og følger opp anbefalte tiltak i etterkant.

Samtidig stiller BDO spørsmål ved at FARTT kun gjennomfører diskusjonsbaserte øvelser. Vi mener det er avgjørende at en driftsleverandør tester beredskap og evne til å håndtere uønskede situasjoner også fra et teknisk ståsted. Aktuelle scenarioer kan være å teste full gjenoppretting av utvalgte kritiske systemer, kritisk infrastruktur og test av gjenoppretting fra backup. Disse testene bør ikke gjøres kun av FARTT sitt driftspersonell isolert, men sammen med andre relevante parter som tjenesteeiere, kriseledelse og et utvalg sluttbrukere.

Det er BDOs oppfatning at handlingsplanene det refereres til i beredskapsplanen ikke er utarbeidet per dags dato. BDO anbefaler at dette gjøres, ettersom konkrete handlingsplaner basert på relevante scenarioer vil øke sannsynligheten for en mer hurtig og korrekt håndtering av hendelser.

7.4 KONKLUSJON

Revisor vurderer at de undersøkte forhold *avviker i noen grad* fra revisjonskriteriene. Selskapet har nylig revidert beredskapsplanverket, men handlingsplaner for utvalgte scenarioer virker ikke å være ferdigstilt. Selskapet gjennomfører evalueringer etter øvelser og hendelser, men har ikke

rutiner for å gjennomføre tekniske øvelser. Dette gjør selskapet sårbart i håndteringen av nye og ukjente hendelser, ref. erfaringer fra hendelsen som inntraff høsten 2022.

7.4.1 Anbefalte tiltak

BDO anbefaler følgende tiltak, i en ikke-prioritert rekkefølge:

- Gjennomføre andre former for øvelser i tillegg til diskusjonsøvelser, herunder tekniske øvelser som omfatter gjenoppretting av utvalgte systemer, infrastruktur og gjenoppretting fra backup. Øvelsene bør involvere andre relevante parter som tjenesteeiere, kriseledelse og et utvalg sluttbrukere.
- Utarbeide handlingsplaner for de utpekte områdene i beredskapsplanen.

8 SAMLET VURDERING OG KONKLUSJON

Det er BDOs samlede vurdering at FARTT har hatt et økende fokus på IT-sikkerhet, men at det gjenstår vesentlige forbedringer for å kunne stadfeste at FARTT har et tilfredsstillende IKT-sikkerhetsnivå.

Gjennomgående for revisjonen er at FARTT har innført forbedringer det siste året, men at det fremdeles er en del avvik sett opp mot NSMs grunnprinsipper for IKT-sikkerhet og anerkjent beste praksis.

Disse avvikene innebærer at FARTT og eierkommunene er sårbare for cyberangrep, og at det ved en større hendelse kan ta lengre tid enn nødvendig å oppdage angrepet, begrense og håndtere skadeomfanget, og gjenopprette systemene.

Denne vurderingen baserer vi på følgende hovedfunn:

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

Basert på dette har vi følgende overordnede hovedanbefalinger til hvordan FARTT bør bedre IKT-sikkerheten for eierkommunene:

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

Mer detaljerte anbefalinger er oppsummert i de enkelte delkapitlene i rapporten.

9 HØRINGSUTTALELSE

9.1 KOMMUNEDIREKTØRENS UTTALELSE

Kommunedirektørene i Tynset, Alvdal, Rendalen, Tolga og Folldal gir i fellesskap følgende uttalelse til rapport IKT-sikkerhet i FARTT.

IKT-sikkerhet er et sentralt område for kommunene. Kommunenes arbeid med overordnet ROS-analyser viser tydelig hvor sårbare vi er dersom vi mister tilgangen på våre IKT-systemer, enten bortfallet skyldes langvarig mangel på strømtilførsel, cyberangrep, nedetid på sentrale systemer, eller andre årsaker.

Hele bredden i den kommunale driften er avhengig av stabile og trygge IT-løsninger i hverdagen. Videre er vi nødt til å ha kontroll på sensitive data, beskytte oss selv mot angrep eller nedetid, ha gode systemer for å oppdage og håndtere hendelser, samt ha gode løsninger for backup og gjenoppretting. Rapporten vil bli et nyttig verktøy for videre arbeid med IKT-sikkerhet.

Etableringen av organisasjonen FARTT hadde blant annet sitt utgangspunkt i å bygge sterkere fagmiljø på sikkerhet. Som rapporten viser, gjøres det mye godt arbeid som er med å bedre IKT-sikkerheten i kommunene, samtidig som det er åpenbare utviklingsområder og konkrete tiltak som må gjennomføres for å være på et godt nok nivå.

Både FARTT selv, styret i FARTT, kommunedirektører og øvrig kommuneledelse må ta del i avklaringer rundt oppfølgning av rapporten. Kommunedirektør har ansvar for internkontroll i egen kommune (herunder IKT-sikkerhet), og dermed blir samhandlingen mellom ledelsen i FARTT og ledelsen i kommunene avgjørende for å lykkes, og for å jevnlig vurdere om status for IKT-sikkerhet er god nok.

Samlet konkluderer rapporten med at det er behov for *vesentlige forbedringer* for å kunne si at kommunene og FARTT har et godt nok nivå på IKT-sikkerhet. Dette er en konklusjon som tas på alvor og som utløser behov for systematisk og samlet innsats umiddelbart.

Rapporten leveres til kontrollutvalgene i kommunene som vil komme med sine anbefalinger til videre oppfølgning. For kommunedirektørene er det naturlig at det videre arbeidet gjøres som en felles prosess mellom kommunene og FARTT gjennom de etablerte styringslinjene, men at hyppigheten og omfanget av samhandling og rapportering forsterkes i den nærmeste perioden.

9.2 FARTTS UTTALELSE

IKT Fjellregionen IKS (omtalt som FARTT) er kjent med rapportutkastet pr 9. august 2023.
Her er vårt svar på rapporten.

Som IKT driftsleverandør, behandlingsansvarlig for egen virksomhet og databehandler for FARTT kommunene så tas rapporten IKT sikkerhet FARTT og arbeidet med informasjonssikkerhet og personvern på det største alvor.

Selskapet har siden starten i 2005 vært del av en enorm IT-utvikling i forhold til ny teknologi, nye systemer og opplever som mange andre aktører et endret risikobilde, som konsekvens av mere komplekse IT-systemer, mere data å håndtere, mere data ut i sky og ikke minst et trusselbilde i stadig endring. FARTT har frem til nå jobbet jevnlig med informasjonssikkerhet og personvern, men erkjenner at dette arbeidet må forbedres fremover, dette viser også rapporten.

Forvaltningsrapporten tar for seg viktige temaer og de ulike problemstillingene viser noe av kompleksiteten i arbeidet med informasjonssikkerhet og personvern. Rapporten tar for seg 5 ulike problemstillinger der det foreligger vurderinger og tiltak.

Vi vil i denne høringen ikke kommentere de enkelte problemstillingene, men vil på generelt grunnlag si at vi prioriterer å rette opp i de feil/mangler som rapporten påpeker, så raskt dette er mulig innafor dagens rammer. Dette arbeidet er allerede igangsatt og vil pågå fortløpende.

FARTT og eierkommunene må jobbe enda tettere sammen om informasjonssikkerhet og personvern, både i forhold til prosesser og systematisk kontroll, men også på generell basis. Selskapet har etter loven sin egen rolle og ansvar, dette gjelder også eierkommunene. Hver for seg skal kravene og regelverk etterleves av den enkelte organisasjon, i samarbeid må vi jobbe hardt for å løse felles utfordringer og problemstillinger slik at dette ivaretas for fellesskapet. Flere problemstillinger vil kunne løses med forholdvis raske tiltak, mens noen problemstillinger vil kreve mere arbeid.

Rapporten peker på noen større problemstillinger, der styret, representantskap og ikke minst eiere må gå i dialog og søke å avklare hvordan de kan ivaretas på best mulig måte. Dette fordi dette berører viktige områder som behov for mere ressurser både i forhold til mannskap, kompetanse og ikke minst økonomi.
Dette mener vi er viktige rammefaktorer som må ivaretas for å dekke behovene.

Vi har valgt å kommentere noe av innholdet i rapporten, direkte i dokumentet. Noe av dette berører faktadelen, men vi mener det er viktig at fakta fremstilles på en riktig måte.

Vi vil også understreke at deler av rapporten er fortrolig informasjon og må unntas offentlighet.

Vi ser på gjennomføring av forvaltningsrevisjonen i FARTT som et viktig redskap for å bli bedre på områder der det er mange komplekse utfordringer. Det ligger mye læring i dette, samtidig som krav og regelverk skal ivaretas. I dette tilfellet skal vi ta vårt ansvar og vi vil jobbe sammen med kommunene for å bli bedre på informasjonssikkerhet og personvern.

Tynset 02.10.2023

Sverre Jenssen

Daglig leder

Kontakt
Jonas Strisland
Senior Associate Consulting

m: +47 975 22 704
e: jonas.strisland@bdo.no