Nasjonal kommunikasjons-myndighet

Tilsynsrapport Telenor

- **hendelser som påvirket nødmeldingstjenesten høsten 2024**

Offentlig sammendrag av sikkerhetsgradert tilsynsrapport (foreløpig)

27. februar 2025

Sammendrag

Dette dokumentet er et offentlig sammendrag av en sikkerhetsgradert tilsynsrapport (foreløpig). Rapporten er å anse som foreløpig da Telenor skal kunne kommentere innholdet, før Nkom fatter et endelig vedtak.

Nasjonal kommunikasjonsmyndighet (Nkom) er tilsynsmyndighet for tilbydere av elektronisk kommunikasjonsnett og -tjenester etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 10-1, jf. § 1-4 og er utpekt som tilsynsmyndighet etter sikkerhetsloven for ekomsektoren, jf. lov 1. juni 2018 nr. 04 om nasjonal sikkerhet (sikkerhetsloven) § 3-1 andre ledd.

Nkom gjennomførte hendelsesbasert tilsyn etter flere uønskede hendelser i Telenor Norge AS sitt nett. Hendelsene rammet blant annet nødmeldingstjenesten 29. august, 16. september, 17.-18. oktober og 13. november 2024. Tilsynets hovedfokus har vært å undersøke hendelsesforløp, bakenforliggende årsaker, konsekvenser, og virksomheten sitt interne arbeid med sikkerhet og beredskap i henhold til ekomloven og sikkerhetsloven med tilhørende forskrifter.

Etter gjennomført tilsyn har Nkom avdekket 22 avvik og tre observasjoner knyttet til blant annet:

- at virksomheten ikke har sikret at sluttbrukere kunne foreta anrop til nødetatenes nødmeldingstjeneste
- at gjennomføring av planlagt arbeid ikke ble gjennomført i tråd med kravene om forsvarlig sikkerhet
- at risikovurdering av nødmeldingstjenesten har vært mangelfull
- at det ikke er gjennomført tilstrekkelig testing, evaluering eller revisjon av nødmeldingstjenesten
- at det på flere områder er mangelfulle eller ikke oppdaterte risiko- og sårbarhetsvurderinger
- at det ikke er tilstrekkelig redundans, dvs. reserveløsninger for tjenester
- at det det ikke er gjort tilstrekkelig revisjon av underleverandør
- at varsling til Nkom ikke har vært rettidig

Virksomheten har fått forhåndsvarsel om pålegg om retting av avvikene og skal utarbeide en tidfestet handlingsplan for lukking av avvikene. Handlingsplanen skal oversendes Nkom og den skal være brutt ned i ulike aktiviteter og delmål som er nødvendige for å gjennomføre korrigerende tiltak.

Formålet med gjennomføringen av tilsynet med virksomheten var å kontrollere at krav etter ekomloven og sikkerhetsloven med tilhørende forskrifter er oppfylt. Tilsynet har ikke kontrollert alle

områder innenfor virksomhetens sikkerhets- og beredskapsarbeid. Virksomheten er selv ansvarlig for å ha forsvarlig sikkerhet i sine kommunikasjonsnett og -tjenester.

Innholdsliste

1 Innledning

Nasjonal kommunikasjonsmyndighet (Nkom) som myndighet i ekomsektoren skal føre tilsyn med at sikkerhetstiltakene hos eiere av nett og tjenester for elektronisk kommunikasjon tilfredsstiller de funksjonelle kravene i eller i medhold av ekomloven.

Nkom har gjennomført tilsyn i medhold av lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 10-1 første ledd første punktum:

«Myndigheten skal føre tilsyn med at krav fastsatt i eller i medhold av loven er oppfylt.»

Videre har Nkom gjennomført tilsyn, som sektormyndighet, i medhold av lov 1. juni 2018 nr. 04 om nasjonal sikkerhet (sikkerhetsloven) § 3-1 andre ledd:

«Departementet kan bestemme at myndigheter med sektoransvar som fører tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur, skal føre tilsyn med virksomheter som er omfattet av loven.»

1.1 Mål for tilsynet

Formålet med gjennomføringen av tilsynet med virksomheten var å kontrollere at krav etter ekomloven og sikkerhetsloven med tilhørende forskrifter er oppfylt. Tilsynet har ikke kontrollert alle områder innenfor virksomhetens sikkerhets- og beredskapsarbeid. Virksomheten er selv ansvarlig for å ha forsvarlig sikkerhet i sine kommunikasjonsnett og -tjenester.

1.2 Lover og forskrifter

Lover og forskrifter som Nkom har ført tilsyn etter:

- Lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven)
- Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven)
- Forskrift 16. februar 2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften)
- Forskrift 16. februar 2004 nr. 426 om nummerressurser for elektroniske kommunikasjonsnett og -tjenester (nummerforskriften)
- Forskrift 10. september 2012 nr. 866 om klassifisering og sikring av anlegg i elektronisk kommunikasjonsnett (klassifiseringsforskrifta)
- Forskrift 7. desember 2011 om autorisasjon for virksomhet som utfører installasjon og vedlikehold av elektronisk kommunikasjonsnett (autorisasjonsforskriften)

- Forskrift 27. september 2005 nr. 1094 om elsikkerhet i elektronisk kommunikasjonsnett
- Forskrift 20. desember 2018 nr. 2053 om virksomheters arbeid med forebyggende sikkerhet (virksomhetssikkerhetsforskriften)

1.3 Gjennomføring av tilsynet

Nkom varslet tilsyn av Telenor etter den første hendelsen 29. august 2024 og har utvidet tilsynet etter hvert som de påfølgende hendelsene fant sted. Tilsynet er gjennomført i form av dokumentgjennomgang, presentasjoner, tekniske undersøkelser, samtaler og intervjuer av nøkkelpersonell hos Telenor og stedlig befaring av anlegg. Nkom har fått støtte fra Direktoratet for Samfunnssikkerhet og beredskap (DSB) i tilsynet for eksperthjelp knyttet til strøm.

Stedlig tilsyn er vanlig å gjennomføre når det er behov for å avklare detaljer, samt for å sikre at Nkom sin forståelse er korrekt. Nkom har ved to anledninger gjennomført stedlig tilsyn:

- 12.-13. november 2024: samtaler og intervju hos Telenor, Fornebu.
- 3.-5. desember 2024: tekniske undersøkelser, samtaler og intervju på anlegg. Samtaler og intervju hos Telenor, Fornebu.

1.4 Tilsynsmetodikk

Tilsynet er gjennomført med utgangspunkt i NS-EN ISO 19011, Veiledning for revisjon av styringssystemer.

Tilsynet er gjennomført ved dokumentgjennomgang, intervjuer, presentasjoner, befaring av anlegg og tekniske undersøkelser for å identifisere revisjonsbevis. Tilsynsmyndigheten vurderer deretter identifiserte revisjonsbevis opp mot bestemmelser i ekomloven og sikkerhetsloven med forskrifter, for videre å avdekke eventuelle avvik eller gjøre observasjoner av relevante forhold.

Avvik: manglende samsvar med bestemmelser i eller i medhold av lov. Dersom avvik avdekkes skal disse korrigeres slik at identifiserte forhold samsvarer med bestemmelser, og slik at identifiserte avvik ikke gjenoppstår – ved å undersøke og fjerne underliggende årsaker.

Observasjoner: beskrivelse av forhold som ikke er avvik, men som tilsynsmyndigheten mener bør påpekes slik at virksomheten kan gjøre endringer for å bedre sikkerheten.

Tilsynsrapporten fokuserer i all hovedsak på forbedringspunkter, dvs. forhold som er i strid med bestemmelser eller nevnte regelverk. Forhold som er i samsvar med regelverket beskrives normalt ikke. Tilsynsrapporten har som mål å bære et bidrag til virksomhetens arbeid med å forbedre

sikkerhetstilstanden i elektroniske kommunikasjonsnett og -tjenester, men danner også grunnlag for videre oppfølging fra tilsynsmyndighetenes side.

1.5 Beste praksis

Endringene i ekomloven av 1. mars 2013 innførte et forsvarlighetsnivå for sikkerhet (ekomloven § 2-10 første ledd). Et slikt funksjonskrav angir hvilket sikkerhetsnivå som skal oppnås, men ikke hvordan det skal oppnås. Dermed må den enkelte virksomhet fastlegge hvordan den konkret skal møte myndighetskravet. I forarbeidene til ekomloven[1] fremgår det at:

«[…] Forsvarlighetsnivået vil utgjøre det pålagte nivået og er ment å ligge over gjeldende krav til nødvendig sikkerhet. Med begrepet «forsvarlig» menes at nett og tjenester skal være tilgjengelige, og at integriteten og konfidensialiteten skal beskyttes. Hva som for øvrig må anses for å være forsvarlig vil fremkomme gjennom markedspraksis, tilgjengelig teknologi og internasjonale krav. Det er tilbyders ansvar at tjenestene som tilbys holder et forsvarlighetsnivå […]».

Det er en rekke eksempler på god markedspraksis (beste praksis) både i form av standarder og praksis fra sikkerhetsarbeid i andre sektorer. Det eksisterer flere standarder for arbeid med kvalitet, sikkerhet og informasjonssikkerhet. Noen av de mest kjente, og som ofte blir benyttet er ISO 27000-serien, ISF Standard of Good Practice, ITIL, ISO 31000, ISO 9001 m.fl. I tillegg finnes det flere organisasjoner som utgir veiledninger på feltet. Nkom ser hen til disse i sin vurdering av hva som kan anses å være forsvarlig sikkerhet for ivaretakelse av kritisk infrastruktur.

Som nevnt vil vurderingen av hva som anses å være forsvarlig fremkomme gjennom markedspraksis, tilgjengelig teknologi og internasjonale krav. I tillegg til å se hen til sektorovergripende regelverk og andre myndighetskrav i andre relevante sektorer, vurderer Nkom forsvarlighetsbegrepet opp mot relevante standarder. Det er i gjennomføringen av tilsynet også blitt vektlagt Nasjonal sikkerhetsmyndighets (NSM) veiledere.

[1] Prop. 69 L (2012-2013) Endringer i ekomloven

2 Hendelsene høsten 2024

I løpet av høsten 2024 har det ved fire tilfeller forekommet uønskede hendelser som har påvirket nødmeldingstjenesten.

29. august 2024

Torsdag 29. august 2024 ble Nkom, gjennom redaksjonell media, gjort oppmerksom på at det var problemer med politiets nødnummer 112. Politiet meldte til media at politidistriktene ikke kunne motta meldinger fra publikum på nødnummer 112. Berørte samtaler ble opplevd som stumme anrop. Feilen medførte at sluttbrukere av Lyse Tele (ICE), Telia og Telenor sine mobilnett ikke kom i forbindelse med politiets operasjonssentraler ved bruk av nødnummer 112. Feilen oppstod i forbindelse med planlagt oppgradering av en tjenesteplattform. Feilen rammet mobilanrop foretatt over 4G til nødnummeret 112 i hele landet i en tidsperiode på 2 timer og 20 minutter.

16. september 2024

Mandag 16. september 2024 feilet tidvis mobilanrop over 4G i Telenors nett mot nødnummer 110 og 112 i hele landet. Anropene ble, som ved hendelsen 29. august 2024, opplevd som stumme anrop av operatørene på nødmeldesentralene. For anrop til nødnummer 113 var feil kun synlig gjennom feil nummervisning for enkelte anrop. Feilsituasjonen ble utløst av problemer knyttet til kommunikasjon mellom nettverkselementer. Dette medførte at prosesser i en tjenesteplattform hang seg opp. Viktig signalering ble dermed ikke tolket korrekt, noe som påvirket talemeldingen. Feilen varte i 56 minutter.

17.-18. oktober 2024

Torsdag 17.-18. oktober 2024 ble anrop fra Telenors abonnenter til nødnummeret 110, 112 og 113 ikke rutet til korrekt geografisk nødmeldesentral. Samtalene ble i stedet rutet til alternativt svarsted, som var nødmeldesentralene i Oslo. Dette fungerte for 110 og 112, men anropsoppsett tok noe lenger tid. For 113 ble anrop rutet til feil nummer, som medførte at innringer mottok en talemelding med beskjed om at nummeret ikke var i bruk. Dette skyldtes en organisatorisk feil ved at nummeret til nødnummeret 113 ikke var endret som det skulle. Feilen varte i 3 timer og 24 minutter.

13. november 2024

Onsdag 13. november 2024 ble det gjennomført vedlikeholdsarbeid på en av Telenors lokasjoner.
I forbindelse med vedlikeholdet ble det gjort en feil som medførte at utstyr mistet tilgang til strøm og derfor slo seg av. Normalt ville ikke dette fått annet enn lokale konsekvenser, men en konfigurasjonsfeil medførte at de redundante løsningene ikke fungerte etter hensikt.

Etter noe tid ble feilen rettet, men da hadde allerede flere tjenester blitt berørt. Dette gjaldt blant annet nødnummertjenester, mobil tale og data, anrop til diverse spesialnummer og fast trådløst bredbånd.

3 Hovedfunn

Etter gjennomført tilsyn med virksomheten har Nkom avdekket 22 avvik og tre observasjoner. Overordnet har Nkom funnet avvik i tilknytning til følgende områder:

- at virksomheten ikke har sikret at sluttbrukere kunne foreta anrop til nødetatenes nødmeldingstjeneste
- at gjennomføring av planlagt arbeid ikke ble gjennomført forsvarlig
- at risikovurdering av nødmeldingstjenesten har vært mangelfull
- at det ikke er gjennomført tilstrekkelig testing, evaluering eller revisjon av nødmeldingstjenesten
- at det på flere områder er mangelfulle eller ikke oppdaterte risiko- og sårbarhetsvurderinger
- at det ikke er tilstrekkelig redundans, dvs. reserveløsninger for tjenester
- at det det ikke er gjort tilstrekkelig revisjon av underleverandør
- at varsling til Nkom ikke har vært rettidig

3.1 Avvik og observasjoner

Det gjennomførte tilsynet har funnet 22 avvik og 3 observasjoner:

- Avvik 1: Migreringen (…)[2] ivaretok ikke i tilstrekkelig grad forsvarlig sikkerhet til nødmeldingstjenesten.
- Avvik 2: Virksomheten sikret ikke at egne sluttbrukere og sluttbrukere tilknyttet andre ekomtilbydere kunne foreta anrop til nødetatenes nødmeldingstjeneste 29. august 2024.
- Avvik 3: Virksomheten sikret ikke at egne sluttbrukere kunne foreta anrop til nødetatenes nødmeldingstjeneste 16. september 2024.
- Avvik 4: Virksomheten sikret ikke at innringers telefonnummer ble overført for alle nødanrop til nødetatenes nødmeldingstjeneste 16. september 2024.
- Avvik 5: Virksomhetens endringshåndtering av nødnummerruting i forkant av hendelsen 17.-18. oktober 2024 ivaretok ikke i tilstrekkelig grad forsvarlig sikkerhet til nødmeldingstjenesten.
- Avvik 6: Virksomheten sikret ikke at egne sluttbrukere 17.-18. oktober 2024 kunne foreta anrop til nødetatenes nødmeldingstjeneste nødnummer 113.
- Avvik 7: Virksomheten sikret ikke at egne sluttbrukere og andre sluttbrukere tilknyttet andre ekomtilbydere kunne foreta anrop til nødetatenes nødmeldingstjeneste 13. november 2024.

[2] del av tittel unntatt jf. offentleglova § 13 jf. forvaltningsloven § 13 første ledd nr. 2

- Avvik 8: Virksomheten overholdt ikke varslingsplikten til Nkom.
- Avvik 9: Mangelfull risikovurdering av nødmeldingstjenesten.
- Avvik 10: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4 og forvaltningsloven § 13 første ledd nr. 2.
- Avvik 11: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4.
- Avvik 12: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4.
- Avvik 13: Mangelfull testing, evaluering og revisjon av nødmeldingstjenesten.
- Avvik 14: Virksomheten har ikke gjennomført revisjon av underleverandør.
- Avvik 15: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4.
- Avvik 16: Virksomheten hadde ikke forsvarlig sikkerhet ved gjennomføring av planlagt arbeid (…)[3].
- Avvik 17: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4.
- Avvik 18: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4.
- Avvik 19: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4.
- Avvik 20: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4.
- Avvik 21: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4.
- Avvik 22: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4.
- Observasjon 1: Det er en risiko for at virksomheten ikke har tilstrekkelige kompetansehevingstiltak for kriseledelsen.
- Observasjon 2: Den er en risiko for at virksomheten ikke øver relevante scenarioer eller vesentlige deler av organisasjonen øves.
- Observasjon 3: Unntatt offentlighet jf. offentleglova § 13 jf. sikkerhetsloven § 5-4.

3.2 Virksomheten sikret ikke at sluttbrukere kunne foreta anrop til nødetatenes nødmeldingstjeneste

Plikten til å sikre muligheten til å anrope nødmeldingstjenesten er en viktig og grunnleggende plikt i ekomregelverket, og denne må ivaretas av ekomtilbyderne. I henhold til ekomloven § 2-6 om anrop til nødmeldingstjeneste og geografisk lokalisering av nødanrop, første ledd første punktum fremgår det at *"[t]ilbyder… skal sikre at sluttbruker kan foreta anrop til nødetatenes nødmeldingstjeneste".*

Bestemmelsen oppstiller dermed både et krav til å implementere en ordning som sikrer anrop til nødmeldingstjeneste, og til å sikre at anrops-ordningen faktisk fungerer. I denne sammenheng vises det også til Prop. 69 L (2012-2013) Endringer i ekomloven s. 101 hvor det fremgår at endringer i bestemmelsen er en presisering og tydeliggjøring av at alle tilbydere har en plikt til å sikre at sluttbruker kan foreta anrop til nødetatenes nødmeldingstjenester.

[3] del av tittel unntatt jf. offentleglova § 13 jf. sikkerhetsloven § 5-4 og forvaltningsloven § 13 første ledd nr. 2

De fire hendelsene medførte at sluttbrukere ikke kunne foreta anrop til nødetatenes nødmeldingstjeneste, og at denne tjenesten dermed ikke var tilgjengelig. Uavhengig av bakenforliggende årsaker og avtaler med brukere, i dette tilfellet nødetatene, er plikten å sikre at sluttbrukere kan foreta slikt anrop.

Det følger videre av nummerforskriften § 18 første ledd at *"[a]lle tilbydere skal sikre at anrop til nødmeldetjenestene kan gjennomføres ved bruk av spesialnumrene 110, 112, 113".*

Ekomloven § 2-6 og nummerforskriften § 18 pålegger tilbyder en klar og tydelig plikt til å sikre at sluttbrukere kan foreta anrop til nødmeldetjenesten og at slikt anrop kan gjennomføres ved bruk av spesialnumrene 110, 112, 113.

For befolkningens grunnleggende trygghet og for akutte nødsituasjoner er det viktig at tilgangen til nødmeldingstjenesten opprettholdes gjennom pålitelige og stabile tjenester. Det foreligger et betydelig skadepotensiale ved nedeperioder dersom befolkningen ikke kommer i kontakt med nødmeldetjenesten gjennom de dedikerte spesialnumrene.

Ved hendelsen 29. august 2024 mottok nødmeldesentralene til nødnummeret 112 stumme anrop som ble sendt over 4G-nettet i en tidsperiode på 2 timer og 20 minutter, slik at nødstilte ikke kunne formidle hva nødsituasjonen gjaldt.

Ved hendelsen 16. september 2024 feilet tidvis anrop over 4G til nødnummeret 110 og 112 i hele landet i 56 minutter. Nødmeldesentralene mottok tidvis stumme anrop, slik at nødstilte ikke kunne formidle hva situasjonen gjaldt.

Ved hendelsen 17.-18. oktober 2024 feilet alle anrop fra virksomhetens kunder til nødnummeret 113 i hele landet i hele 3 timer og 24 minutter.

Ved hendelsen 13. november 2024 var det periodevis lange samtaleoppsett av varierende lengde og enkelte stumme anrop til nødmeldingstjenesten.

Et stumpt anrop er ikke et anrop i lovens forstand. Lange samtaleoppsett på inntil 50 sekunder oppleves også i praksis som at nødmeldingstjenesten var utilgjengelig for innringer og nødstilte.

3.3 Virksomheten har ikke hatt forsvarlig sikkerhet ved gjennomføring av planlagt arbeid

Tilsynet har avdekket at Telenor ikke har gjennomført planlagt arbeid på forsvarlig vis. Tilsynet har også avdekket at Telenor ikke har hatt forsvarlig sikkerhet ved gjennomføring av planlagt arbeid knyttet til nødmeldingstjenesten. Det betyr blant annet at selskapet ikke har hatt tilstrekkelig kontroll på at oppgaver er utført korrekt, at ansvar ikke er overført når personell har sluttet og at de ikke godt nok har vurdert mulige konsekvenser av det planlagte arbeidet.

3.4 Virksomhetens risikovurdering av nødmeldingstjenesten har vært mangelfull

Virksomheten har opplyst at målbildet for nødmeldingstjenesten er at den skal være oppe til enhver tid, og at det grunnleggende rasjonale bak arkitekturen for nødnummer er å redusere risikoen for utfall ved å ha back-up alternativer for hvert steg i anropshåndteringen. Nødnummertjenesten har blitt utviklet i mange år i samarbeid med nødetatene, og den er blitt endret gradvis i takt med modernisering av nettet. Det er gjennom tilsynet avdekket at virksomheten har ikke utarbeidet en risikovurdering som dekker hele verdikjeden i nødmeldingstjenesten.

3.5 Virksomhetens testing, evaluering eller revisjon av nødmeldingstjenesten er ikke gjennomført tilstrekkelig

Det er under tilsynet ikke fremlagt dokumentasjon på systematisk gjennomføring av testing, evalueringer eller revisjoner av nødmeldingstjenesten. Virksomheten opplyste at det ikke er et system for å gjennomføre jevnlige evalueringer eller revisjoner av verdikjeden for nødanrop, utover ved større endringer i ekomnettet. Virksomheten har opplyst at det arbeides med å organisere jevnlige tverrfaglige revisjoner av nødnummertjenesten. Den mangelfulle gjennomføringen av testing, evaluering og revisjon av nødmeldingstjenesten er etter Nkoms oppfatning ikke i henhold til god bransjepraksis og ivaretar ikke i tilstrekkelig grad forsvarlig sikkerhet til tjenesten.

3.6 Virksomheten har på flere områder ikke oppdaterte eller mangelfulle risiko- og sårbarhetsvurderinger

Nkom har i forbindelse med tilsynet pålagt virksomhetene å utlevere dokumentasjon, herunder flere relevante risiko- og sårbarhetsvurderinger. Flere av de oversendte risikovurderingene er av eldre dato, og/eller mangelfulle. Både ekomloven og sikkerhetsloven med tilhørende forskrifter stiller krav til at tilbyder regelmessig skal gjennomføre vurdering av risiko. Det er en forutsetning at risikovurderinger gjennomføres med tilstrekkelig dekning og er oppdaterte nok til å danne grunnlag for iverksetting av forebyggende, og beredskapsmessige, sikkerhetstiltak, med forsvarlig sikkerhet som resultat.

Endringer i forhold som påvirker status på verdiene det gjennomføres risikovurdering i forhold til, og i trusselbildet gjennom de siste årene, som blant annet er omtalt i EOS-tjenestenes årlige trusselvurderinger, er etter Nkoms mening faktorer som må reflekteres i virksomhetens risikovurderinger.

3.7 Det har ikke vært tilstrekkelig redundans for tjenestene

Telenor har ikke sørget for at det er tilstrekkelig redundans, dvs. reserveløsninger for tjenestene. Det innebar for eksempel at hendelsen 13. november 2024 fikk større konsekvenser enn den ville ha hatt, dersom reserveløsninger hadde fungert slik de skulle.

3.8 Virksomheten har ikke gjort tilstrekkelig revisjon av underleverandør

Det er etter Nkoms vurdering ikke gjort en tilstrekkelig revisjon av underleverandør som har en avgjørende rolle i verdikjeden. Det er viktig at slike revisjoner gjennomføres for å sikre at underleverandørene følger opp krav og at de gjennomfører gode risikovurderinger knyttet til oppdragene.

3.9 Virksomheten har ikke varslet rettidig

Tilbydere av ekomnett og -tjenester skal varsle Nkom uten ugrunnet opphold, og senest innen en halv time etter at tilbyder er kjent med hendelsen, om hendelser som vesentlig kan redusere eller har redusert tilgjengeligheten til ekomtjenester.

Formålet med bestemmelsen om varsling er å sikre at Nkom får tilstrekkelig informasjon på et tidligst mulig tidspunkt til å kunne vurdere behovet for oppfølging av hendelsen og iverksetting av eventuelle ytterligere sikkerhets- og beredskapstiltak. Nkom har ansvaret for det overordnede situasjonsbildet på tvers av tilbyderne i ekomsektoren, og å koordinere dette situasjonsbildet og -forståelse med andre myndigheter. For å kunne agere og iverksette hensiktsmessige tiltak, herunder for eksempel koordinering og videre varsling til myndighetsorganer med beredskapsansvar for andre sektorer, er det derfor viktig at Nkom varsles raskt om utfall av elektroniske kommunikasjonsnett og -tjenester. Det er spesielt viktig når varslene omhandler uønskede hendelser som kan påvirke understøttelsen av grunnleggende nasjonale funksjoner.

Den enkelte ekomtilbyder, herunder virksomheten, vil ikke besitte et komplett situasjonsbilde som ivaretar myndighetenes, og det norske samfunnets, behov for informasjon. I tillegg til potensielt andre sammenfallende hendelser, eksempelvis i en tilspisset sikkerhetspolitisk situasjon.

4 Oppfølgning av tilsyn

Det gjennomførte tilsynet har funnet 22 avvik og tre observasjoner. Det er sendt varsel om vedtak om pålegg om lukking av avvikene. Virksomheten skal utarbeide en tidfestet handlingsplan for korrigering av alle avvik og oversende handlingsplanen til Nkom. Handlingsplanen skal være brutt ned i ulike aktiviteter og delmål som er nødvendig for korrigeringen, og den skal være forpliktende og resultere i at alle avvikene blir korrigert.

Avvikene skal lukkes i tre steg[4] :

1. Avvikene i de områdene det er gjennomført tilsyn på må lukkes.
2. Virksomheten må kontrollere at det ikke finnes tilsvarende avvik på områder som ikke ble omfattet av tilsynet. Hvis det finnes tilsvarende avvik, må disse korrigeres.
3. Virksomheten må identifisere de bakenforliggende årsakene til at avviket kunne oppstå, og gjøre korrigerende tiltak slik at tilsvarende avvik ikke kan oppstå igjen.

Underveis i prosessen skal virksomheten, basert på handlingsplanen, rapportere til Nkom på korrigeringen av avvik og eventuelle forsinkelser i henhold til handlingsplanen. I forbindelse med lukking av avvik skal virksomheten, som en del av korrigeringen, sørge for å oppbevare tilstrekkelig dokumentasjon om hvordan avvikene har blitt korrigert slik at det sikres notoritet i arbeidet. Samtidig påpeker Nkom at utarbeidelse av en tidfestet handlingsplan ikke skal forhindre at arbeidet med å korrigere dele av avvikene starter umiddelbart for å redusere risiko.

Telenor er gitt frist til 1. juni 2025 med å utarbeide en tidfestet handlingsplan for korrigering av virksomhetens avvik.

[4] jf. NS-EN ISO 9001:2015 Ledelsessystemer for kvalitet – Krav som beskriver en slik måte for lukking av avvik