Tekniske løsninger for nødmeldingstjenste

Nasjonal kommunikasjonsmyndighet

Tekniske løsninger for nødmeldingstjeneste

SAMMENDRAG

I perioden fra august til november 2024 har flere kritiske hendelser knyttet til nød-nummertjenestene i Norge (110, 112 og 113) synliggjort ulike sårbarheter i dagens tekniske infrastruktur. Disse hendelsene, som har ulike rotårsaker, har påvirket publikums mulighet til å kontakte nødetatene og vist alvoret og konsekvensene av sårbarhetene. På bakgrunn av dette har Nkom iverksatt tilsyn som inkluderer en helhetlig gjennomgang av alle hendelsene. Denne rapporten er imidlertid ikke en del av selve tilsynet, men har som formål å beskrive dagens tekniske løsning på et overordnet nivå, vurdere erfaringer fra andre europeiske land og identifisere muligheter for forbedring av tilgjengelighet og robusthet for nødnummertjenestene i Norge.

Dagens løsning for nødnummertjenester i Norge baserer seg på en delvis sentralisert infrastruktur der all trafikk sendes til Telenor før den videreformidles til korrekt mottakssted/ nødmeldesentral. Denne modellen sikrer en konsistent behandling av nødanrop, men skaper samtidig en sårbar avhengighet som kan føre til alvorlige konsekvenser ved nettverks- eller tjenestefeil hos Telenor. Avhengigheten til Telenors kjernenett innebærer at et utfall i viktige nettverks- og/eller tjenesteplattformer vil gjøre nødnumre utilgjengelig for hele befolkningen – selv om andre tilbyderes transport- og mobilnett fungerer. Hendelsene med nødnummer høsten 2024 understreker behovet for en mer robust og desentralisert infrastruktur for nødnummertjenestene i Norge.

Nkom har vurdert ulike måter for å øke robustheten for nødnummertjenestene. Den nye europeiske spesifikasjonen for nødnummertjenester, Next Generation 112 (NG112), er et godt alternativ for å gjøre nødnummertjenesten i Norge mer motstandsdyktig og sikker. Etablering av NG112-funksjonalitet vil redusere sårbar-heten og styrke samfunnets evne til å håndtere kritiske hendelser. Nkom har innhentet informasjon på hvilke løsninger andre land har. Flere land har en tilsvarende modell som Norge, men er i ferd med å vurdere eller innføre nye og mer robuste løsninger.

Nkom anbefaler å legge til rette for at flere tilbydere kan koble nødanrop direkte til nødetatene, og på sikt etablere NG112-funksjonalitet. Dette samsvarer med inter-nasjonale standarder for nødkommunikasjon mellom innringer og nødetat, og forbedrer kvaliteten og muligheten for informasjonsutveksling mellom nødmeldesentralene. Det er viktig at det offentlige går foran og stiller krav til sikkerhet og robusthet ved anskaffelser av kritiske tjenester. Nkom anbefaler at innføring av ny robust løsning for nødnummertjenesten gjennomføres med god samhandling mellom myndigheter, nødetater og tilbydere. For å sikre en god og rask fremdrift anbefaler Nkom at dette organiseres som prosjekt på samme måte som ved innføringen av befolkningsvarsling på mobil.

INNHOLD

Nasjonal kommunikasjons-myndighet

1 INNLEDNING

I perioden august til november 2024 har det vært flere kritiske hendelser knyttet til feil på nødnummer-tjenestene i Norge (110, 112 og 113). Disse hendelsene har hatt ulike rotårsaker, men felles for alle er at de har påvirket befolkningens mulighet til å kontakte nødetatene og dermed svekket samfunnets evne til å håndtere kriser og ulykker effektivt.

I løpet av fire måneder har det vært utfordringer med nødnumrene ved fire separate anledninger:

- **29. august 2024:** Feilen varte i omtrent 2,5 timer og resulterte i stumme anrop, fordelt mellom ulike operatører. Problemet oppsto i forbindelse med planlagt arbeid i Telenor sitt nett.

- **16. september 2024:** I løpet av én time ble anrop til 110 og 112 berørt av stumme anrop, mens nødnummeret 113 opplevde problemer med nummervisning. Problemet oppsto i forbindelse med planlagt arbeid i Telenor sitt nett og følgende inkonsistens mellom nettverkselementer.

- **17.-18. oktober 2024:** En feil hos Telenor førte til at anrop ble rutet feil geografisk, eller ikke kom gjennom til nødnumrene. For 110 og 112 fungerte omrutingen til alternativt svarsted (Oslo), men det tok noe lenger tid å sette opp anropet. For 113 fungerte ikke dette. Problemene varte i over tre timer.

- **13. november 2024:** Det er fremdeles ikke helt klart hva den underliggende feilen var, men foreløpige analyser viser til at det var strømbrudd internt i en av sentralene til Telenor. Dette skapte ulike feil i Telenors mobile kjernenett, og problemene varte i omtrent seks timer.

Hendelsene viser behovet for økt robusthet og pålitelighet i kritisk kommunikasjonsinfrastruktur.

Feilene har avdekket sårbarheter i systemene og rutinene, noe som krever en grundig gjennomgang og forbedring. Nkom har satt i gang tilsyn som omfatter alle de nevnte hendelsene. Tilsynet innebærer gjennomgang av dokumentasjon, undersøkelser av infrastruktur og intervjuer for å avdekke fakta og identifisere forbedringspunkter i henhold til ekomloven og tilhørende forskrifter.

Ekomloven regulerer pliktene til tilbydere av elektronisk kommunikasjon (ekom) når det gjelder nødanrop og sikkerhetskrav for ekomnett og -tjenester. Ifølge ekomloven § 2-6 må tilbydere av elektroniske kommunikasjonstjenester sørge for at sluttbrukere kan ringe nødetatene. Plikten gjelder de tilbydere av elektronisk kommunikasjonstjeneste som tilbyr sluttbruker en tjeneste som gir mulighet for å foreta innenlandsk anrop til ett eller flere nummer i den nasjonale nummerplanen. Plikten til dynamisk og statisk opprinnelsesmarkering og nød-SMS er nærmere regulert i ekomforskriften § 6-2 a og b. Nummerforskriften § 18 pålegger tilbydere å sikre at nødanrop kan gjennomføres ved bruk av spesialnumrene 110, 112 og 113. Videre har tilbyderne etter ekomloven § 2-10 plikt til å tilby elektronisk kommunikasjonsnett og -tjeneste med forsvarlig sikkerhet for brukerne i fred, krise og krig, samt opprettholde nødvendig beredskap, og prioritere viktige samfunnsaktører ved behov.

Resultatene fra tilsynet skal bidra til å styrke sikkerhetstilstanden i elektroniske kommunikasjonsnett og -tjenester og danner grunnlag for videre oppfølging fra myndighetenes side.

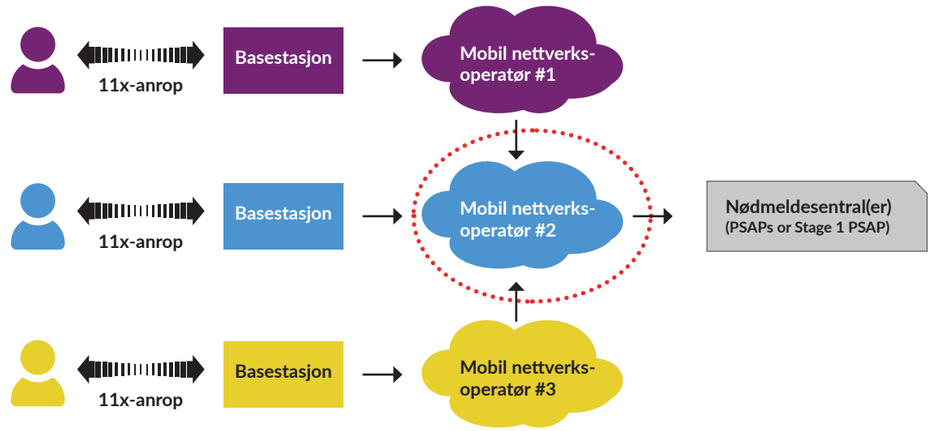
Nkom har på bakgrunn av hendelsene undersøkt hvordan nødnummertjenestene kan organiseres på en mer sikker og robust måte. Hovedformålet med denne rapporten er å gi en overordnet beskrivelse av dagens tekniske løsning, gi en oversikt over løsninger i andre europeiske land, og identifisere muligheter for å forbedre tilgjengeligheten og robustheten til nødnummertjenestene i Norge.

2 DAGENS TEKNISKE LØSNING FOR NØDNUMMER I NORGE

Nødanropene er en essensiell kommunikasjonskanal for publikum når de skal varsle nødmeldesentralene (Public Safety Answering Points, PSAPs), og det er avgjørende at disse tjenestene fungerer som forventet. Det er en grunnleggende forventning i befolkningen at slike anrop til enhver tid lar seg gjennomføre.

Helse, brann og politi har per i dag ulike kommunikasjonsoppsett. Helse har i sin AMK-sentral (akuttmedisinsk kommunikasjonssentral) gått over fra ISDN (analog kommunikasjon) til et IP-basert kommunikasjonsoppsett, noe som kan begrense avhengigheten til en enkelt operatør og muliggjøre en mer fleksibel infrastruktur. Videre har de startet arbeidet med å integrere elementer av ESInet (Emergency Services IP Network) i sin nye kommunikasjonsløsning, inkludert sentralisert kontroll og funksjonalitet fra NG112 (se kapittel 3 for mer informasjon om ESInet og NG112). Politi og brann er fortsatt på eldre kommunikasjonsløsning med ISDN internt i nødmeldesentralene, men har planer om å oppgradere til IP-baserte løsninger i relativt nær fremtid.

I Norge er det tre nasjonale mobilnettoperatører; Telenor, Telia og Ice/Lyse Tele (heretter referert som tilbydere). Telenor har den største kundemassen med ca. 2,54 millioner mobilkunder, og deretter Telia og Ice med henholdsvis 2,08 millioner og 0,94 millioner kunder. I dag rutes alle nødanrop fra mobiltelefoner og IP-telefoni til 110, 112, eller 113 (til sammen refereres disse som 11X) via Telenor på termineringssiden - uavhengig av hvilken tilbyder anropene kommer fra (Figur 1).



Figur 1: Infrastrukturen er i dag bygget opp slik at all trafikk knyttet til nødnummer (11X) rutes via Telenor (Mobil nettverksoperatør #2), dette uavhengig av hvilken mobilnettoperatør anropene kommer fra.

Systemene til Telenor er i hovedsak likt for brann, politi og helse Telenor har en intern "nødetat web" hvor all viktig informasjon om nødetatene er samlet, som adresser, numre og kontaktpersoner.

Når man ringer 11X konverteres anropene til riktige «langnummer» (dvs. 8-sifret nummer til nærmeste nødmeldesentral) basert på innringerens lokasjon/kommunenummeret der aktuell basestasjon er lokalisert, slik at de kan rutes til rett nødmeldesentral. Ansvaret for denne konverteringen ligger hos tilbyderen (Telenor, Telia, Ice) som håndterer innringerens/kundens anrop, dvs. tilbyderen anropet originerer fra.

Anropet overføres så til Telenor som deretter håndterer rutingen av samtalene til den rette nødetaten og lokasjonen. Rent teknisk skjer dette ved at anropet transporteres via Telenor sitt eget nett, frem til den relevante nødmeldesentralen. Hver nødmeldesentral har redundante VPN-forbindelser fra Telenor sin tjenesteplattform og inn til sin egen lokasjon. Telenor overvåker disse og har rutiner og prosedyrer for å sikre at anrop kommer frem, selv ved tekniske feil eller hendelser som gjør at en nødmeldesentral besluttes evakuert.

Dette innebærer altså en to-delt løsning for anrop til 11X, hvor den tilbyderen det ringes fra (originerende) ruter samtalen til Telenor, som håndterer terminerings-siden, det vil si overtar samtalen og sender den videre til korrekt nødmeldesentral. De reelle numrene til samtlige nødmeldesentraler hører altså til i Telenor sitt nett og er å betrakte som bedriftskunder hos Telenor.

For dagens løsning, der all trafikk til nødmeldesentralene rutes via Telenor sitt nett, skisseres følgende styrker og sårbarheter:

Styrker ved dagens løsning:

- Telenor har en intern "nødetat web" med all viktig informasjon om nødmeldesentralene, noe som gir effektivitet og nøyaktighet når de skal sikre at trafikk kommer frem til riktig sted. Dette vil også gjøre det relativt enkelt å realisere nødvendige endringer, ettersom dette da kan gjøres på ett sted.
- Telenor håndterer og terminerer alle nødanrop uavhengig av teleoperatør, noe som sikrer enhetlig og konsistent behandling.
- Telenor overvåker egne samband og har rutiner for backup og prosedyrer for å sikre at anrop kommer frem, selv ved feil eller dersom en nødmeldesentral blir evakuert.
- Nødmeldesentralene har kun én part å forholde seg til når det gjelder feilmeldinger og andre forhold. Det samme gjelder oppgraderinger og videreutvikling av hvilke datasett som skal fra innringer/bruker, og til nødmeldesentralene.

Sårbarheter ved dagens løsning:

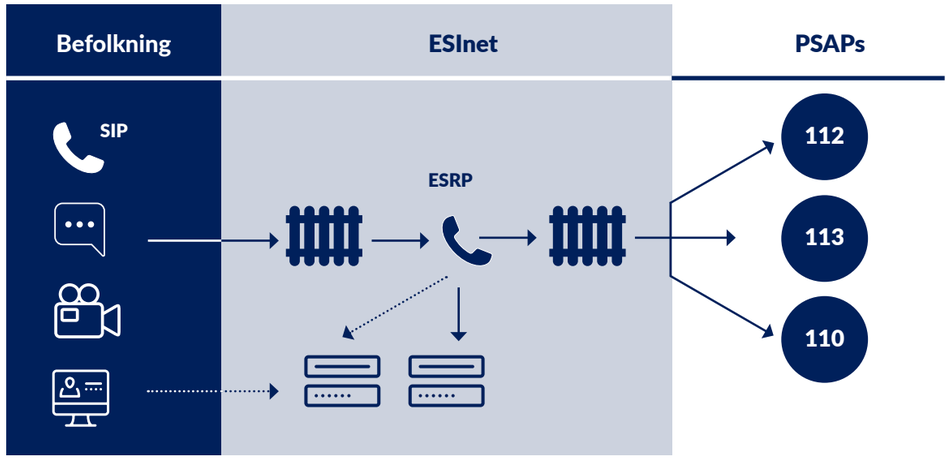
- Dersom Telenor har problemer med sine nett, tjenester og/eller linjer, kan dette i ytterste konsekvens medføre at ingen nødanrop kan gjennomføres i hele landet.
- Planlagt arbeid, vedlikehold og oppgraderinger (PAIN) i Telenor sitt nett kan føre til midlertidige avbrudd eller redusert kapasitet, noe som kan påvirke tilgjengeligheten av nødtjenestene for hele befolkningen.

3 FREMTIDENS TEKNISKE LØSNING FOR NØDNUMMER

Next Generation 112 (NG112) er en moderne plattform for nødsamband basert på Internett-protokoll (IP-teknologi) som støtter «komplett samtale» *(Total Conversation)*. Dette betyr at det er mulig for innbyggere å kontakte nødetatene via ulike kommunikasjonsmåter som tekst *(RTT - Sanntidstekst)*, video og lokasjonsdata, i tillegg til tradisjonelle telefonsamtaler. Denne sammensetningen av informasjon gir personellet hos nødetatene flere måter å motta kritisk informasjon på, og gjør systemet mer tilgjengelig for innringere/nødstilte med nedsatt hørsel eller andre funksjonsnedsettelser. Kombinasjonen av tale, tekst og video styrker også nødmeldesentralenes beslutningsgrunnlag.

ESInet (Emergency Services IP Network) er et IP-basert nettverk som muliggjør utvekslingen av tale, video og tekstdata som i sum utgjør arkitekturen for NG112. ESInet er ansett av EENA (European Emergency Number Association) som anbefalt metode for å sikre redundant og standardisert kommunikasjon mellom innringer/nødstilt, tilbyder og nødmeldesentralene (Figur 2). ESInet gjør blant annet at mest mulig presis informasjon om hvor innringer befinner seg oversendes til den mest relevante nødmeldesentralen, noe som er viktig for å yte effektiv bistand fra nødetatene. Nødanrop kan også rutes til alternative sentraler (det vil si 110, 112 eller 113) ved overbelastning eller tekniske problemer ved en av dem.

Venstre side av figur 2 viser at befolkningen kan kontakte nødmeldesentralene via IP-telefoni (SIP), tekstmeldinger og video, og at posisjonsdata leveres fra nettverket. Meldinger og samtaler rutes inn i ESInet som sørger for korrekt ruting av nødanropet gjennom flere noder:



Figur 2: Viser hvordan nødanrop rutes gjennom ESInet (Emergency Services IP Network) til de offentlige nødmeldesentralene (PSAPs).

- ESRP (Emergency Services Routing Proxy): Ruter anropet til riktig sted.
- LIS (Location Information Server): Lagrer posisjonsdata for å identifisere anropets plassering.
- ERCF (Emergency Call Routing Function): Bruker posisjonsdata for å bestemme riktig nødmeldesentral (PSAP) anropet skal sendes til.

Høyre side av figur 2 viser at den riktige nødmeldesentralen (PSAP) mottar anropene basert på innringers plassering og type anrop.

ESInet er et privat og overvåket IP-nett som knytter sammen de ulike elementene (tekst, tale, posisjon og video). Enkelt forklart kan en si at et ESInet sørger for å knytte sammen kjernekomponentene (som tale, video og tekstdata) som trengs for å kunne realisere såkalt «komplett samtale» (Total Conversation).

Det finnes flere alternativer for å bygge slike nett: enten kan hver tilbyder eller nødetat sette opp sitt eget, de kan lage et felles design, eller det kan etableres av en tredjepart. Den umiddelbare fordelen er at flere mobilnett og internettleverandører kan koble seg til, og man kan unngå sårbarheter ved at kun en enkelt tilbyder har ansvar alene for å sende nødanrop frem til korrekt nødmeldesentral. Man sikrer dermed at tilgang til nødmeldetjenester blir *uavhengig av ett enkelt nett*. Avhengig av design, kan også tilbydere bruke hverandre for å fremsende nødanrop dersom det er feil i et nett. ESInet sikrer utvidet redundans og høy sikkerhet for både nettoperatør og nødmeldesentraler ettersom dette er en del av det grunnleggende designet.

NG112 skal sikre at alle nødnumre blir universelt tilgjengelige og tilbyr tjenester som sanntidstekst og GNSS-basert posisjonering (Global Navigation Satellite System). Per nå er det kun helse (ved HDO) som har gjort betydelige fremskritt her. Politi og brann har med NG112-konseptet i sine kravspesifikasjoner, som utgangspunkt for leveranse av sine fremtidige kommunikasjonsløsninger.

Dagens kommunikasjon med nødmeldesentralene skjer nesten utelukkende gjennom tale, med noe bruk av video i 110 -og 113-tjenestene (uavhengige/frittstående tjenester som ikke er spesielt integrert med øvrige systemer for hendelseshåndtering), samt tekst for enkelte brukergrupper («NødSMS»). En rikere og standardisert multimediebasert kommunikasjon, inkludert sanntidsvideo, kan bidra til at hendelser håndteres raskere og mer effektivt, i tråd med samfunnets utvikling mot mer integrerte og avanserte kommunikasjonsformer som «komplett samtale» og mer sømløs informasjonsdeling mellom nødmeldesentralene.

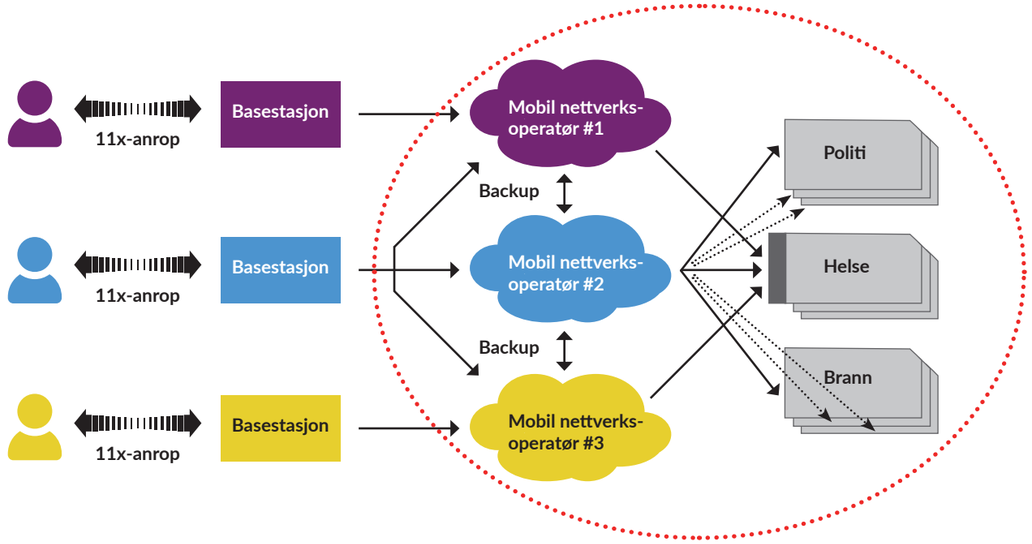
4 VURDERING AV LØSNINGER

Nkom har inntrykk av at både helse, politi og brann vurderer ESInet og en IP-basert løsning som viktige for fremtidig robusthet og sikkerhet. Dette er spesielt relevant med tanke på dagens sikkerhetspolitiske situasjon, hvor tilbydere er mulige mål for hendelser som truer sikkerheten.

Helsetjenestens driftsorganisasjon for nødnett (HDO), Politiets IT-enhet (PIT), Direktoratet for Samfunnssikkerhet (DSB) og beredskap/ Branns Driftsorganisasjon (BDO), samarbeider og diskuterer tekniske løsninger og mulige anbefalinger til videre oppgradering av kommunikasjonssystemene. Det vil være mulig for nødmeldesentralene å fase inn den nye løsningen med ESInet gradvis, hvor helse kan gå foran og teste ut den nye arkitekturen. Dette vil gi en mulighet til å høste erfaringer som de andre etatene kan dra nytte av.

4.1 MULIG ALTERNATIV PÅ KORT SIKT

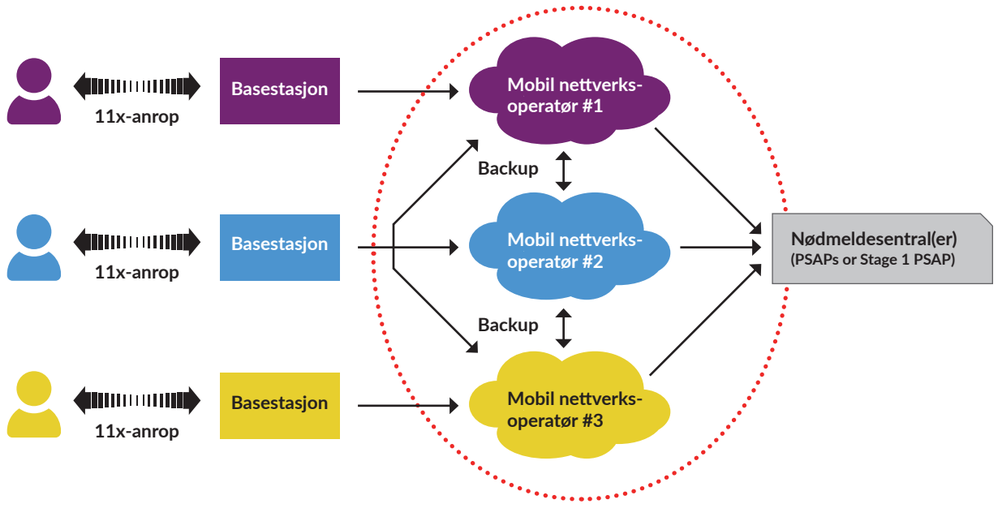
Helse har etablert et datasenter som en type front-end-mottak av innkommende nødanrop. Figur 3 illustrerer hvordan helse kan ha forbindelse med hver tilbyder inn til sitt felles mottak, og at de fra dette mottaket selv ruter trafikken til korrekt nødmeldesentral. Ettersom politi og brann per nå mangler et slikt sentralisert mottak, og er avhengige av at hver nødmeldesentral kobles direkte opp mot tilbyder(e), ville det i dagens struktur måtte etableres et svært stort antall forbindelser (én til hver enkelt nødmeldesentral for både 110 og 112, pluss redundans for hver av disse). Basert på dette er det sannsynligvis mest hensiktsmessig for brann og politi å beholde en løsning som tilsvarer dagens frem til de har etablert et IP-basert kommunikasjonsoppsett tilsvarende det helse har.



Figur 3: Alternativ løsning som trolig kan etableres i dag.

Helse er godt posisjonert for å ta i bruk en IP-basert og ESInet-kompatibel kommunikasjons-løsning, men dette avhenger av at også politi og brann gjør tilsvarende oppgraderinger. Merk også at enkelte tjenester innenfor NG112 krever at mobiloperatørene gjør nødvendige endringer i sine nett, eksempelvis for å kunne tilby sanntids-tekst (RTT – Real Time Text).

En løsning på kort sikt kan innebære at alle tilbydere med egne nettverk (Telenor, Telia og Ice) knytter seg direkte til de rette instansene/nødetatene for mottak av nødnummer. På denne måten frigjøres nødetatene fra ensidig avhengighet til Telenor (Figur 4). Fordi det blir et stort antall logiske forbindelser som må etableres er dette ikke et godt alternativ for den enkelte nødmeldesentral før alle nødmeldesentralene har et IP-basert kommunikasjonsoppsett.



Figur 4: Alle mobilnettoperatører sender direkte til nødetatene uten å være avhengig av Mobil nettverks operatør #2.

I løsningen der alle tilbyderne sender direkte til nødmeldesentralene, skisseres følgende styrker og sårbarheter:

Styrker ved at alle tilbyderne sender anrop direkte til rett nødmeldesentral:

- Økt robusthet: Ved å inkludere flere tilbydere fjernes risikoen for at et landsdekkende utfall i Telenors nett påvirker alle nødanrop.

- Bedre tilgjengelighet: Anrop kan rutes gjennom andre operatører dersom én operatør opplever problemer.

- Løsningen følger europeiske spesifikasjoner for fremtidens nødkommunikasjon (NG112).

- Nødetatene har en langt bedre infrastruktur for deling av data og mulighet for å «overta for hverandre» dersom utfall eller andre problemer tilsier at det er nødvendig.

Sårbarheter ved at alle tilbyderne sender anrop direkte til rett nødmeldesentral:

- Økt kompleksitet: Flere operatører involvert kan øke kompleksiteten i drift og feilsøking. Dette stiller krav til mottaksleddet om tilstrekkelig kompetanse på IT og telekom.

- Kostnader: Implementeringen av en ny løsning vil kreve betydelige investeringer fra både operatører og nødetater for å sikre kompatibilitet og redundans.

- Koordinering: Det vil være behov for tettere koordinering mellom flere aktører, noe som kan komplisere drift, vedlikehold og utvikling.

Ved å implementere løsningen der alle tilbyderne sender nødanrop direkte til nødmeldesentralene kan en oppnå økt robusthet og bedre tilgjengelighet, samtidig som internasjonale spesifikasjoner følges. Likevel må man være oppmerksom på økt kompleksitet, kostnader og behovet for tettere koordinering.

4.2 FREMTIDIG LØSNING

Norge har en tredelt struktur i nødetatenes nødmeldesentraler, med ulik organisering og teknologi. EENAs (European Emergency Number Association) foreslåtte “inside out approach” legger strategien først, deretter infrastrukturen (her ESInet), og til slutt integrering av mobilaktører, tjenester, app-leverandører og IoT-aktører.
En slik styringsmodell kan danne en ramme for arbeidet med NG112, som i hovedsak gjelder kommunikasjon fra innringer/nødstilt til nødmeldesentralen (men også kommunikasjon/informasjonsutveksling nødmeldesentralene imellom vil kunne bli bedre, inkludert deling av informasjon og muligheten for å etablere en felles situasjonsforståelse).

Fordelene med NG112 inkluderer raskere respons gjennom sanntids posisjonsdata og multimedia. Dette gir nødetatene mer sammensatt informasjon fra meldingsmottak i nødmeldesentralene til videre tiltak utover i de ulike organisasjonene, noe som forbedrer beslutningstakingen. Økt tilgjengelighet og robust kontinuitet gjennom distribuerte nettverk gir også gevinst. Samtidig innebærer overgangen kostnader for infrastruktur og opplæring, samt strenge krav til koordinering, datasikkerhet og personvern.

NG112 representerer en betydelig forbedring i nødkommunikasjon ved å integrere tale, tekst og video, noe som gjør systemet mer tilgjengelig og effektivt. Ved å benytte ESInet og LIS, sikres nøyaktig posisjonsinformasjon og robust kommunikasjon mellom innringer/nødstilt og nødmeldesentraler. Implementeringen av NG112 i Norge vil kreve nøye planlegging og koordinering, men vil med stor sannsynlighet styrke bered-skapen og sikkerheten for befolkningen.

5 ANDRE LANDS LØSNINGER FOR NØDNUMMER

Nkom har sendt ut en forespørsel til utvalgte europeiske land for å få en oversikt over deres løsninger. I e-posten, datert 25.10.24, ba vi om informasjon om selve kommunikasjonsløsningen, samt styrker og sårbarheter ved disse. Nkom mottok svar fra Nederland, Portugal, Ungarn, Belgia, Sverige og Frankrike. Svarene er oppsummert som følger:

Nederland:
Nederland bruker i dag samme løsning som Norge, men planlegger å gå over til systemer med flere tilbydere i løpet av neste år. Dette vil øke robustheten, men også kompleksiteten og kravene til ekspertise.

Portugal:
Portugal benytter også samme løsning som Norge, men oppgraderer nå sine nødmeldesentraler til å følge NG112-spesifikasjonen. Dette vil forbedre deres system og øke robustheten.

Ungarn:
Ungarn bruker samme løsning som Norge, men planlegger å gå over til et system med flere tilbydere i løpet av neste år. Dette for å gi en mer robust løsning.

Belgia:
Belgia har nylig opprettet en sekundær rute inn til nødmeldesentralene, slik at to tilbydere nå håndterer trafikken. Tidligere hadde de samme løsning som Norge med én tilbyder, men etter et utfall av nødnummeret i september 2023, har de sikret kontinuerlig drift med en ekstra tilbyder.

Sverige:
I Sverige termineres nødanrop fra fire forskjellige tilbydere til SOS Alarm (et slags «front-end» mottak), et offentlig eid selskap som håndterer anrop til 112, som er felles nødnummer for helse, politi og brann (slik som det er vanlig å gjøre det i Europa). Sverige rapporterer ingen klare sårbarheter med sin løsning. En styrke er at de har egne nummerserier, uten å måtte kjøpe dem fra andre tilbydere. Fra et tilgjengelighetsperspektiv er det ingen negative aspekter, men løsningen er dyrere enn å bruke én tilbyder, både når det gjelder infrastruktur, administrasjon, service og support.

Frankrike:
I Frankrike terminerer alle tilbyderne direkte til nødetatene. Frankrike fremhever redundans som en av fordelene med løsningene. En ulempe som nevnes er at det er mange operatører som må ha informasjonen om konverteringsnumrene (konvertering fra 112 til «langnummer» for den enkelte nødmeldesentral).

Løsningen i Portugal, Ungarn og Nederland ligner den norske, med én tilbyder. En svakhet ved denne løsningen er mangelen på alternative ruter ved utfall, noe som kan være kritisk. Flere innganger øker robustheten, men også kompleksiteten og kravene til kompetanse.

> *"Dagens løsning for nødnummer er ikke robust nok. Vi må, som de andre landene i Europa, bort fra at vi har avhengighet til en enkelt tilbyder.*
>
> Svein Sundfør Scheie
> sikkerhetsdirektør i Nkom

6 NKOMS ANBEFALING

I dag er alle nødanrop sentralisert via Telenor, noe som gir en konsistent håndtering av anropene, men innebærer en tydelig sårbarhet dersom Telenor får problemer i sitt nett. Dette understreker behovet for å vurdere alternative løsninger som kan øke tilgjengeligheten, robustheten og påliteligheten. Dette er også i samsvar med det som gjøres i andre europeiske land.

Nkom anbefaler at det etableres ESInet med NG112-funksjonalitet hos alle nødetatene. NG112 vil være mer robust og i tråd med internasjonale standarder for nødkommunikasjon. Nkom ser at NG112-løsningen kan gi et vesentlig løft i nødkommunikasjonens robusthet, kvalitet og sikkerhet i Norge. For å nå dette målet kreves det god samhandling mellom myndigheter, nødetater og tilbyderne. Arbeidet bør organiseres etter modell fra befolkningsvarsling på mobil (Nødvarsel på mobil).

Å innføre den tekniske løsningen i henhold til NG112 kan ta noe tid. Helse (113) har kommet lengst av de tre nødetatene når det gjelder teknisk infrastruktur og mulighet for å etablere forbindelse med hver enkelt tilbyder. Det anbefales derfor på kort sikt at helse etablerer en slik forbindelse med hver enkelt tilbyder. Dette krever at også Telia og Lyse Tele/Ice må etablere systemer for håndteringen og leveranse av nødanrop, uavhengig av Telenor.

Besøksadresse: Nygård 1, Lillesand
Postadresse: Postboks 93, 4791 Lillesand
Tlf: 22 82 46 00
nkom.no