Post- og teletilsynet
Norwegian Post and Telecommunications Authority

Se adresseliste

Vår ref.:1203644-156 - 004
Vår dato: 17.11.2014

Deres ref.:
Deres dato:

Saksbehandler: Runar Langnes

Informasjon fra Post- og teletilsynet til norske kommuner

Post- og teletilsynet (PT) har utarbeidet informasjon som vi ønsker å nå ut til beredskapskontaktene i norske kommuner med på en effektiv måte. PT henvender seg derfor til Fylkesmennene og deres beredskapsorganisasjon med ønske om bistand til videre distribusjon. Det dreier seg om en veileder for kommuner i robust elektronisk kommunikasjon og en orientering om prioritet i mobilnett. Begge deler er kort forklart nedenfor, og de to aktuelle dokumentene som vi ønsker distribuert, følger vedlagt.

Ekomveileder for kommuner

Norske kommuner er, som ledd i kommunal beredskapsplikt, pålagt å utarbeide helhetlige risiko- og sårbarhetsanalyser (ROS) og PT har utarbeidet en veileder som er ment som støtte til ekomdelen av en ROS. Den inneholder generelle råd om robuste ekomløsninger og om tiltak når vanlige ekomtjenester er utilgjengelige.
Veilederen kan lastes ned fra PTs hjemmesider, se http://www.npt.no/teknisk/sikkerhet-og-beredskap/r%C3%A5d-til-brukere/veileder-for-kommuner.

Prioritet i mobilnett

Brukere med særlig samfunnsviktige oppgaver kan fra 1. juli 2014 få prioritetsabonnement i mobilnett. Prioriterte brukere får bedre fremkommelighet i mobilnettene når kapasiteten i nettene er sprengt. Fylkesmennenes beredskapsorganisasjon og nøkkelpersonell innenfor kommunal beredskap vil være aktuelle kandidater for ordningen. Kommuner og andre virksomheter må søke om godkjenning hos PT før de kan tegne prioritetsabonnement hos sin tilbyder.

Post- og teletilsynet
Besøksadresse / Office address:
Nygård 1, Lillesand

Postadresse / Postal address:
Postboks 93
4791 LILLESAND
NORWAY

Tel +47 22 82 46 00
Fax +47 22 82 46 40
firmapost@npt.no

NO 974 446 871
www.npt.no

Mer om ordningen og veiledning om hvordan en går fram for å få prioritetsabonnement finnes på PTs hjemmesider www.npt.no. Ved å søke på nøkkelordet «prioritet» vil en få denne lenken øverst http://www.npt.no/forbruker/sikkerhet/prioritet-i-mobilnett/prioritet-i-mobilnett.

Med hilsen

Torstein Olsen
direktør

Einar Lunde
avdelingsdirektør

Vedlegg:
Prioritet i mobilnett – orientering til kommunene
Ekomveileder

1. januar 2015 endrer PT navn til Nasjonal kommunikasjonsmyndighet

Mottaker	Kontaktperson	Adresse	Poststed	Land
Fylkesmannen i Aust-Agder		Serviceboks 606	4809 ARENDAL	
Fylkesmannen i Aust-Agder	Dag Auby Hagen	Serviceboks 606	4809 ARENDAL	
Fylkesmannen i Buskerud	Bente Nyegaard Fjell	Postboks 1604	3007 DRAMMEN	
Fylkesmannen i Buskerud		Postboks 1604	3007 DRAMMEN	
Fylkesmannen i Finnmark		Statens Hus	9815 VADSØ	
Fylkesmannen i Finnmark	Ronny Schjelderup	Statens Hus	9815 VADSØ	
Fylkesmannen I Hedmark	Knut Anders Fossum	Parkgaten 64	2317 HAMAR	
Fylkesmannen I Hedmark		Parkgaten 64	2317 HAMAR	
Fylkesmannen i Hordaland		Postboks 7310	5020 BERGEN	
Fylkesmannen i Hordaland	Arve Meidell	Postboks 7310	5020 BERGEN	
Fylkesmannen i Møre og Romsdal	Kjetil Matvik Foldal	Fylkeshuset	6404 MOLDE	
Fylkesmannen i Møre og Romsdal		Fylkeshuset	6404 MOLDE	
Fylkesmannen i Nordland		Statens hus Moloveien 10	8002 BODØ	
Fylkesmannen i Nordland	Jan Martin Skoglund	Statens hus Moloveien 10	8002 BODØ	
Fylkesmannen i Nord-Trøndelag	Per Arne Stavnås	Postboks 2600	7734 STEINKJER	
Fylkesmannen i Nord-Trøndelag		Postboks 2600	7734 STEINKJER	
Fylkesmannen i Oppland		Postboks 987	2626 LILLEHAMMER	
Fylkesmannen i Oppland	Asbjørn Lund	Postboks 987	2626 LILLEHAMMER	
Fylkesmannen i Oslo og Akershus	Johan Løberg Tofte	Postboks 8111 Dep.	0032 OSLO	
Fylkesmannen i Oslo og Akershus		Postboks 8111 Dep.	0032 OSLO	
Fylkesmannen i Østfold		Postboks 325	1502 MOSS	
Fylkesmannen i Østfold	Espen Pålsrud	Postboks 325	1502 MOSS	
Fylkesmannen i Rogaland	Reidar Johnsen	Postboks 59	4001 STAVANGER	
Fylkesmannen i Rogaland		Postboks 59	4001 STAVANGER	
Fylkesmannen i Sogn og Fjordane		Statens hus Sogn og Fjordane Njøsavegen 2	6863 LEIKANGER	
Fylkesmannen i Sogn og Fjordane	Haavard Stensvand	Statens hus Sogn og Fjordane Njøsavegen 2	6863 LEIKANGER	
Fylkesmannen i Sør-Trøndelag	Dag Otto Skar	Postboks 4710, Sluppen	7468 TRONDHEIM	
Fylkesmannen i Sør-Trøndelag		Postboks 4710, Sluppen	7468 TRONDHEIM	

Fylkesmannen i Telemark		Postboks 2603	3702 SKIEN
Fylkesmannen i Telemark	Jan W. Jensen Ruud	Postboks 2603	3702 SKIEN
Fylkesmannen i Troms	Per Elvestad	Postboks 6105	9291 TROMSØ
Fylkesmannen i Troms		Postboks 6105	9291 TROMSØ
Fylkesmannen i Vest-Agder		Postboks 513 Lundsiden	4605 KRISTIANSAND S
Fylkesmannen i Vest-Agder	Yngve Årøy	Postboks 513 Lundsiden	4605 KRISTIANSAND S
Fylkesmannen i Vestfold	Jan Helge Kaiser	Postboks 2076	3103 TØNSBERG
Fylkesmannen i Vestfold		Postboks 2076	3103 TØNSBERG
Sysselmannen på Svalbard		Postboks 633	9171 LONGYEARBYEN

Post- og teletilsynet
Norwegian Post and Telecommunications Authority

Prioritet i mobilnett – orientering til kommunene

Brukere med særlig samfunnsviktige oppgaver kan fra 1. juli 2014 få prioritetsabonnement i mobilnett. En abonnent som har prioritet, vil ha større sikkerhet for å komme gjennom enn andre abonnenter når det er høy belastning eller problemer i mobilnettene. Det følgende er en orientering til norske kommuner om ordningen og om hvordan man går frem for å få et slikt abonnement.

Formål med prioritet

Formålet med prioritet i mobilnettene er å gi brukere med ansvar for kritiske samfunnsfunksjoner bedre fremkommelighet i mobilnettene i en krisesituasjon. Kritiske samfunnsfunksjoner er her definert som ivaretakelse av samfunnets og befolkningens grunnleggende behov, som f. eks. mat, vann, varme, sikkerhet og helse. Nøkkelpersonell innenfor kommunal beredskap faller klart inn under ordningen.

På www.npt.no finnes en ikke uttømmende liste over typer virksomheter som kan godkjennes for prioritetsabonnement.

Hvor mange kan få prioritet?

Prioritet i mobilnett er en meget begrenset ressurs som er reservert for inntil 10.000 brukere. Det er derfor nødvendig å ha kontroll over tegning av prioritetsabonnement. PT legger opp til en tillitsbasert forvaltning, og virksomheter som søker om godkjenning må samtykke i visse betingelser. Blant annet skal prioritetsabonnement opprettes utelukkende for de personer/funksjoner i virksomheten som har et tydelig beredskapsmessig behov for mobiltelefoni, og som det vil være særlig viktig at får gitt beskjeder osv. i en unntakssituasjon,

PT har definert foreløpige tildelingsrammer[1] for ulike sektorer. Disse er basert på behovsanalyse fra Direktoratet for samfunnssikkerhet og beredskap. En kvote på 4000 enkeltabonnement er satt av til kommuneledelse. Tallet er veiledende og den enkelte kommune og kommunale virksomhet må i utgangspunktet selv vurdere hva slags beredskapsansvar og -behov de har. PT ber om at eget behov vurderes restriktivt. Merk at ordningen er tilpasset de som har behov for å kunne ringe ut, ikke de som først og fremst skal kunne nås.

[1] *Summen av alle delkvotene er noe høyere enn 10000, mens totalt antall samtidige abonnement er begrenset til 10000*

Post- og teletilsynet
Besøksadresse / Office address:
Nygård 1, Lillesand

Postadresse / Postal address:
Postboks 93
4791 LILLESAND
NORWAY

Tel +47 22 82 46 00
Fax +47 22 82 46 40
firmapost@npt.no

NO 974 446 871
www.npt.no

Hvordan fungerer prioritet i mobilnett?
Anrop fra et prioritert nummer vil bryte andre samtaler når det er manglende kapasitet i nettene, men anropet vil ikke bryte nødsamtaler. Prioriteten gjelder ikke innkommende samtaler fra et vanlig abonnement, kun når man ringer ut.

Et prioritert nummer har i tillegg gjesting (roaming) i andre norske mobilnett enn der man selv er kunde. Dette vil si at telefoner med slikt abonnement vil søke seg mot et annet mobilnett og bruke dette, når man er utenfor dekning av «eget» mobilnett[2]. På denne måten er muligheten for å få sin samtale gjennom styrket, selv når det er omfattende problemer i et nett. Dette skjer automatisk, og prioritetsfunksjonen står alltid på.

Både prioritet for utgående samtaler og gjesting i annet nett ved utfall skjer uten at brukeren må foreta seg noe spesielt. Merk at prioriteten kun gjelder for taletrafikk, ikke for datatjenester, og bare i Norge.

Når er prioritet nyttig?
Prioritet i mobilnett er særlig nyttig når svært mange bruker mobilnettet i et lite område samtidig, og slik skaper overbelastning. Typiske situasjoner er store lokale eller regionale ulykker, eller hendelser der mange samtidig belaster mobilnettene ekstra i et bestemt område.

Uvær kan føre til redusert kapasitet i mobilnett, oftest som følge av strømbrudd og ødelagte fiberkabler. Ekstremvær av en ukes varighet har vært et dimensjonerende scenario for ordningen. Sannsynligheten for en slik hendelse er stor, og konsekvensene vil føre til et behov for at utvalgte brukere har prioritet i mobilnett. Andre aktuelle scenarioer er for eksempel terrorhandlinger, stor ulykke (brann, eksplosjon, transportulykke), strålingsfare, naturkatastrofer (skred, skogbrann), omfattende strømutfall og pandemi.

Nødnettet, som nå ferdigstilles over store deler av landet, er det primære kommunikasjonsverktøyet for nødetatene. Prioritet i mobilnett for denne gruppen er kun ment som et supplement. For andre ledere med beredskapsansvar, og særlig i den fasen hvor gjenoppbygging og normalisering er hovedoppgavene, vil tilgang til mobilkommunikasjon være essensielt. Nasjonal kriseledelse, Fylkesmannens beredskapsorganisasjon og kommunal kriseledelse er aktuelle eksempler. Å opprettholde og reetablere kritiske samfunnsfunksjoner i denne fasen av en unntakssituasjon er ett av de viktigste formålene med ordningen.

For å sikre at de utvalgte numrene prioriteres når en kritisk hendelse oppstår, er funksjonaliteten påslått til enhver tid. Risikoen for forsinkelser og feil dersom ordningen skulle slås på etter en

[2] *Merk at på samme måte som ved internasjonal gjesting, er en avhengig av at gjestenettet er i stand til å kontakte ens hjemmenett*

myndighetsbeslutning i hvert enkelt tilfelle, er vurdert å være for høy. Det er derfor en viss risiko for at enkelte uprioriterte samtaler kan bli brutt også i andre situasjoner med overbelastning enn kriser. PT anser denne risikoen og konsekvensene for akseptable.

Opprette prioritetsabonnement

Før en virksomhet, dette tilfellet en kommune eller kommunal virksomhet med samfunnsviktig funksjon, tegner prioritetsabonnement hos en mobiltilbyder, må den søke om godkjenning hos PT. Søknaden sendes via Altinn.no. Innlogging skal skje på vanlig måte med personnummer. Personen som søker, må ha registrert en rettighet i Enhetsregisteret til å fylle ut og sende inn på vegne av virksomheten.

Søknad om godkjenning trenger en bare å sende én gang. I søknaden angir en hvor mange enkeltabonnement virksomheten søker for.

Virksomheten kan etter et positivt vedtak i PT bestille prioritetsabonnement hos sin mobiltilbyder, som kontrollerer mot PTs register at virksomheten er godkjent.
Prioritetsabonnement tilbys mot en løpende årsavgift som fastsettes av mobiltilbyder.
Man kan beholde sin vanlige mobil og sitt mobilnummer, men må ha nytt simkort.

Les mer om fremgangsmåten på PTs hjemmeside www.npt.no. Søk på nøkkelordet «prioritet» og lenke[3] til den aktuelle teksten kommer øverst på siden. Vi tar gjerne imot spørsmål og forslag til forbedringer.

Lillesand, 17. november 2014

1. januar 2015 endrer PT navn til Nasjonal kommunikasjonsmyndighet

[3] *http://www.npt.no/forbruker/sikkerhet/prioritet-i-mobilnett/for-virksomheter*

Post- og teletilsynet
Norwegian Post and Telecommunications Authority

Robust elektronisk kommunikasjon

- veiledning og råd til kommuner

November 2014

1. januar 2015 endrer PT navn til
Nasjonal kommunikasjonsmyndighet

Innhold

1 Om veilederen

Post- og teletilsynet (PT) arbeider for å sikre brukere i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester. Som et ledd i dette gir PT råd til andre myndigheter og brukere om elektronisk kommunikasjon (ekom). I denne veilederen vil kortformen ekom bli brukt.

Kommuner er pålagt å gjennomføre risiko- og sårbarhetsanalyser (ROS). Denne veilederen er ment som støtte til ekomdelen av en ROS.

De første kapitlene i veilederen gir bakgrunnsinformasjon, mens de konkrete rådene finnes i de siste kapitlene.

Kapittel 2 handler om ekom som en sentral del av kommuners helhetlige ROS. For bedre å kunne identifisere sårbarhetene og hvilke tiltak som kan bidra til å sikre tilgang til ekom, er det nyttig å forstå hvordan ekominfrastrukturen er bygd opp. Kapittel 3 gir derfor en kort innføring i ulike ekomnett. Kapittel 4 handler om de vanligste årsakene til bortfall av ekomtjenester.

Kapittel 5 inneholder praktiske råd for valg av robuste ekomløsninger. Til slutt er PTs råd for å forberede seg på kommunikasjonsbehovet i krisesituasjoner samlet i kapittel 6.

Mange kommuner forvalter en betydelig intern ekominfrastruktur. Veilederen har ikke som formål å gi råd om denne, men avgrenser seg til råd som gjelder bruk av de offentlige ekomnettene, som mobil- og bredbåndsnett. Noen kommuner, vanligvis de største, må forventes å være profesjonelle bestillere av ekomtjenester. Denne veilederen er primært ment for de mange kommunene som har få egne ressurser på ekomområdet. PTs mål med veilederen er å hjelpe norske kommuner med å *redusere sannsynligheten for å miste all ekom,* ved å sette dem i stand til på forhånd å gjøre informerte valg.

Veilederen legger vekten på *tilgjengelighet* av ekom. Andre sider ved sikker ekom er også viktige, som at informasjon som sendes ikke blir kjent for uvedkommende (konfidensialitet) eller at informasjonen ikke blir endret underveis (integritet). Dette er imidlertid ikke vektlagt i denne veilederen, heller ikke informasjon om priser.

2 ROS i kommunene

Samfunnet er helt avhengig av tilgang til ekomtjenester. Stadig flere grunnleggende funksjoner, som strøm, vann, helse, samferdsel, finans etc. forutsetter at ekomnett, -tjenester og -utstyr virker nær sagt overalt og hele tiden.

Kommunene har ansvaret for viktige tjenester til innbyggerne og for beredskapsfunksjoner i samfunnet. De er i økende grad avhengig av fungerende ekom både for å levere tjenestene og ivareta funksjonene. Dessuten er ekom nødvendig for effektiv kommunikasjon med befolkningen.

Kommunene er, som ledd i kommunal beredskapsplikt, pålagt å utarbeide helhetlige ROS. Kommunal beredskapsplikt er hjemlet i §§ 14 og 15 i Sivilbeskyttelsesloven. Direktoratet for samfunnssikkerhet og beredskap (DSB) har påpekt at *bortfall av ekomtjenester skal inkluderes i ROS-analyser og planverk og det skal planlegges for alternative løsninger ved bortfall. Dette gjelder lokalt, regionalt og sentralt nivå*. Dette går fram av en rapport[1] som DSB skrev sammen med PT med bakgrunn i erfaringer fra ekom-hendelser i 2011. I oppfølgingen av den samme rapporten har DSB utarbeidet en veileder[2] i helhetlig risiko- og sårbarhetsanalyse i kommuner.

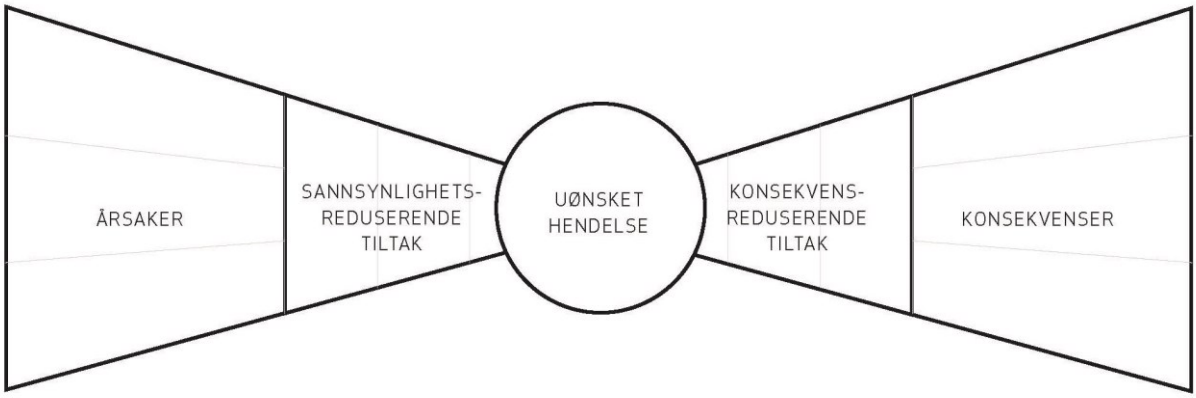
Når kommuner gjennomfører en ROS som involverer ekom, må de avgjøre hvilken risiko de kan akseptere når det gjelder utfall av ekom. Hvor mange minutter, timer eller dager kan kommunens tjenester være uten ekom før situasjonen går ut over viktige samfunnsfunksjoner? Dersom analysen viser at risikoen er for høy, må man treffe tiltak for å redusere risikoen til akseptabelt nivå. Disse tiltakene faller i to kategorier:

1. De som reduserer *sannsynligheten* for at fullstendig utfall inntreffer og
2. de som reduserer *konsekvensene* når fullstendig utfall likevel skjer.

Denne veilederen gir først og fremst råd om tiltak i den *første* kategorien. Uansett hvor mye ressurser som brukes på å sikre tilgang til ekom, vil det likevel alltid være en restrisiko for totalt bortfall av tjenester. Kommuner må derfor ta forholdsregler også for å redusere konsekvensene hvis dette skulle skje. Tiltak i den siste kategorien kan omfatte manuelle rutiner og utradisjonelle kommunikasjonsløsninger. I den generelle

[1] Samfunnets sårbarhet overfor bortfall av elektronisk kommunikasjon (DSB 2012)
[2] http://www.dsb.no/no/Ansvarsomrader/Regional-og-kommunal-beredskap/Aktuelt-Regional-og-kommunal-beredskap/veileder-for-ROS-analyse-i-kommunen/

figuren nedenfor vil uønsket hendelse for en kommune, i denne settingen, være *totalt bortfall av ekom*.
De ROS-faglige begrepene i figuren benyttes i liten grad i rapporten, men man gjenfinner meningsinnholdet ved at vanlige årsaker er beskrevet i kapittel 4, sannsynlighetsreduserende tiltak i kapittel 5 og noen konsekvensreduserende tiltak i kapittel 6.



Figur 1: Et sløyfediagram illustrerer innholdet i en ROS.

3 Hva er ekom?

Elektronisk kommunikasjon, ekom, er i dag så selvfølgelig at vi knapt nok tenker over hva det er eller hvilke nett og tjenester vi bruker. Som brukere forholder vi oss oftest til taletjenester og ulike dataapplikasjoner. Eksempler på det siste kan være alt fra enkle apper på mobilen til systemer som kontrollerer kritiske produksjonsprosesser. Tjenestene forutsetter en underliggende elektronisk kommunikasjon for å fungere. En teknisk definisjon er at *elektronisk kommunikasjon er overføring av informasjon ved hjelp av signaler i fritt rom eller kabel*. Brukere av ekomtjenester får overført signalene av en tilbyder som sørger for at disse flyter til og fra brukeren.

3.1 Ekomnett

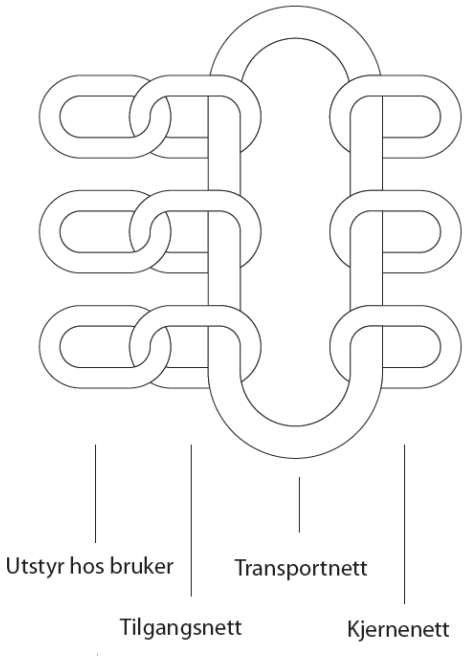
Et ekomnett er produksjonsmaskineriet som formidler ekomtjenester til brukerne. For enkelhets skyld kan vi her dele ekomnett inn i tre hoveddeler:

- Tilgangsnettet
  Tilgangsnettet er den delen av nettet som brukeren er tilknyttet. I mobilnettene er det basestasjoner som utgjør tilgangsnettet, for fast telefoni og bredbånd er det de lokale fiber- eller kobberkablene foruten utstyr i endesentraler. Imidlertid har nettene ofte ingen eller få alternative veier et stykke videre inn i nettene og derfor er det hensiktsmessig å inkludere også denne delen[3] i begrepet tilgangsnett.
- Kjernenettet
  I kjernen av nettene har tilbyderne utstyr hvor viktige deler av tjenesten produseres. Eksempler er utstyr som analyserer det telefonnummeret man ringer til eller den adressen man klikker på i nettleseren. Dette utstyret og forbindelsene mellom dem kan vi kalle kjernenettet.
- Transportnettet
  Det som knytter tilgangsnettene og kjernedelen sammen. Transportnettet er i all hovedsak basert på fiber og er relativt godt sikret mot strømutfall og brudd på enkeltlinjer. I denne framstillingen betrakter vi transportnettet som ett enhetlig nett og én felles ressurs for all ekom.

I tillegg til disse tre delene ekomnettene kan deles inn i, må utstyret som brukeren har ansvaret for, også tas med i en helhetlig beskrivelse. Dette er telefoner, modemer, rutere, datamaskiner og annet utstyr som kommuniserer med ekomnettene.

[3] Ofte kalt «backhaul» i fagterminologi

Figuren nedenfor illustrerer kjeden av elementer som setter en bruker i stand til å kommunisere. Lest fra venstre mot høyre, skal kjeden forstås som leddene som forbinder en bruker på venstre side med ekomtjenester på høyre side. De tre nett-kategoriene over og brukerens eget utstyr er symbolisert ved ledd i en kjede. De horisontale kjedene, skal forstås som alternative forbindelser som benytter ulike nett. Alle figurene i resten av veilederen, har denne figuren som referanse. Merk at figurene ikke er ment å illustrere hvordan kommunikasjon skjer ende til ende.



Figur 2: Kjetting er valgt som metafor for forbindelsen mellom brukeren og ekomtjenestene. Leddene til venstre (brukerutstyr) kan for eksempel være en mobiltelefon, et rutermodem for bredbånd, en fasttelefon. Neste ledd (tilgangsnett) kan være basestasjonene til Telenor, TeliaSonera, ICE, fiber fra Altibox, kobberkabel/DSL fra Telenor mm. Transportnettet er symbolisert ved en stor og kraftig lenke som er felles for nettene. Leddene lengst til høyre (kjernenett) kan for eksempel være der hvor Tele2, TeliaSonera eller Ventelo produserer sine mobiltjenester eller hvor ulike Internett-tilbydere leverer tilknytning til Internett.

Som abonnent av ekomtjenester, er det andre kategorier nett en må forholde seg til. Vi vil derfor gi en innføring i disse og relatere de til modellen over. Fastnett, mobilnett og satellittnett er de hovedtypene nett som gir tilgang til ulike telefoni- og datatjenester. Teknologiene er forskjellige og de representerer ulike tilgangsnett og i noen grad også ulike kjernenett. Transportnettet er imidlertid en felles ressurs for alle bakkebaserte[4] nett.

[4] Dvs nettene som ikke er satellittnett. Merk at også noen satellittnett er avhengige av installasjoner på bakken og dermed ofte også transportnettet.

3.2 Fastnett

I fastnettet er brukeren koplet til med kabel eller via radiolinje. Kabelen eller radiolinjen går fra huset bygningen der brukeren er og frem til nærmeste telesentral, der signalene sendes videre innover i nettet. Det er flere tilbydere som leverer fastnett i Norge, for eksempel er det en rekke lokale selskap som bygger og leverer fibertilknytning til boligområder og bedrifter. Telenors fastnett er likevel det mange forbinder med fastnettet, og dette har tradisjonelt vært bygget på kobberteknologi og sørget for fasttelefoni til de fleste av landets husstander og bedrifter. Dette nettet er under modernisering, men Telenors forpliktelse til å levere tilgang til offentlig telefontjeneste er ikke endret. På kobbernettet til Telenor leveres også bredbånd og bredbåndstelefoni fra andre leverandører. Tradisjonell fasttelefoni og fast bredbåndstelefoni kan altså ha samme tilgangsnett, men tjenestene produseres i ulike kjernenett.

Noen ekomtilbydere tilbyr overføringskapasitet eller faste samband. Det kan være alt fra fiberpar uten noe utstyr i endepunktene til raffinerte produkter med spesifisert kapasitet, kvalitet og robusthet. Mange lokale tilbydere kan ha stor markedsandel i sitt område. På landsbasis er Telenor og Broadnet de største aktørene. Et fast samband kan gå gjennom både tilgangsnettet og transportnettet hvis det er lang avstand mellom endepunktene.

Mange kommuner har flere lokasjoner som skal knyttes sammen. Da er virtuelle private nett (VPN) en vanlig løsning. VPN innebærer at en på en åpen infrastruktur, for eksempel Internett, har sitt eget private nett med mekanismer som sikrer kapasitet og konfidensialitet. Også mobile forbindelser kan inngå i noen typer VPN.

3.3 Mobilnett

I et mobilnett går signalene trådløst mellom mobiltelefonen eller annet brukerutstyr og en basestasjon. Basestasjonen er igjen koplet med kabel eller radiolinje til kjernedelen av ekomnettet. Dette vil si at signalene går i kabler i bakken eller stolper det meste av strekningen mellom to som kommuniserer, og at også mobilnettene vil være utsatt for skader for eksempel ved storm eller ras, akkurat slik som fastnettet.

Det er fire offentlige mobilnett i Norge[5], nettene til Telenor, TeliaSonera (NetCom), Tele2 og ICE. De tre første leverer både kombinerte abonnement for telefoni og datatjenester og særskilte bredbåndsabonnement. ICE leverer (pr. høsten 2014) bare data-abonnement og har en annen type teknologi i nettet enn de tre andre. Telenor og TeliaSonera har landsdekkende nett, mens Tele2 (pr. høsten 2014) har eget nett i deler av landet og bruker ellers enten Telenors eller TeliaSoneras nett der de ikke selv har dekning. Flere mindre mobilselskaper leier tilgang i de store selskapenes mobilnett. Derfor kan man kjøpe abonnement fra en liten tilbyder, og likevel få tilgang til netteierens dekning.

Mobilnettene er innbyrdes uavhengige både i tilgangsnett og kjernenett. Mobiltjenestene produseres på annet utstyr i kjernenettet enn fasttelefoni og fast bredbånd og er i stor grad uavhengige av disse.

3.4 Satellittnett

Når man ringer via et satellittnett**,** går signalene mellom satellittelefonen og en eller flere satellitter som kretser rundt jorda. Man må ha egne telefoner for å bruke dette nettet, og antall brukere som kan kommunisere samtidig er relativt begrenset.

Det er to typer satellitter for satellittelefoni:
1) Geostasjonære satellitter
Disse er plassert i en fast posisjon over ekvator, i en høyde som gjør at de når så langt nord som til Svalbard. Men selv langt sør i Fastlands-Norge, vil det være problematisk å motta signalene nede i daler. Områder hvor det ikke er fri sikt til satellitten ligger i såkalt satellittskygge.

Når kommunikasjonen skjer via geostasjonære satellitter, er tidsforsinkelsen på mellom et halvt og ett sekund. Dette gjør løsningen mindre egnet for tale. Også visse former for datakommunikasjon vil være problematisk på grunn av forsinkelsen.

Inmarsat[6] er nok den største og mest brukte operatøren som tilbyr mobiltjenester via geostasjonære satellitter. En annen tilbyder er *Thuraya*[7], og deres håndholdte telefoner kan i tillegg kommunisere gjennom GSM-nettet.

[5] Dette gjelder pr. høsten 2014. Oppkjøp og konsolideringer kan endre bildet
[6] http://www.inmarsat.com/
[7] http://www.thuraya.com/

2) Lavbanesatellitter

Disse består av satellitter som går i baner rundt jorda og med en omløpshastighet på noen få timer. Det vil normalt til en hver tid være en eller flere satellitter i synsfeltet over oss, slik at satellittskygge sjelden er et problem med denne type system. Lavbanesatellittene danner et nettverk, og signalene går fra en satellitt til en annen før den sendes videre enten til en annen satellittelefon eller en jordstasjon som mottar signalene og videresender disse inn i et bakkebasert ekomnett.

Innenfor denne satellittypen er disse de vanligste:

Iridium[8] består av 66 operative lavbanesatellitter og kan betraktes som et mobilsystem med 66 basestasjoner som går i bane rundt jorda og gir global dekning med en håndholdt terminal. Systemet har relativt liten forsinkelse på signalet, fordi disse satellittene går i kun 800 km høyde over jorda. Den maksimale kapasiteten i et område på størrelse med Sør-Norge vil variere mellom 80 og 240 samtidige brukere. Systemet har svært begrenset kapasitet for datatrafikk. Dersom noen da samtidig bruker data, vil det drastisk redusere kapasiteten for samtaler. Iridium er basert på 90-talls teknologi og har sammenlignbare ytelser med GSM.

Globalstar[9] er en annen operatør av lavbanesatellitter. 40 satellitter går i bane rundt jorda i ca. 1400 km høyde i dette systemet. I motsetning til Iridium-systemet er det ikke kommunikasjon mellom satellittene, noe som betyr at signalene må gå via en jordstasjon før det rutes videre i det offentlige telenettet eller Internett.

[8] https://www.iridium.com/default.aspx
[9] https://eu.globalstar.com/en/

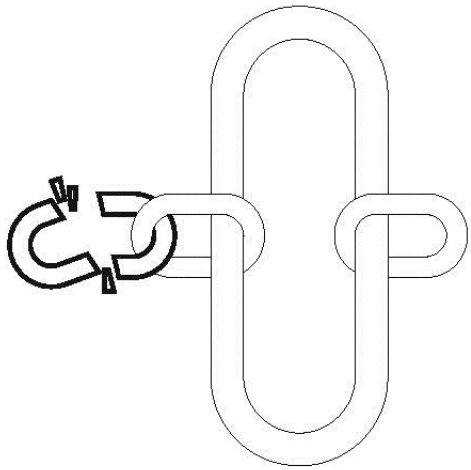
4 Hva kan gå galt?

Risiko- og sårbarhetsanalyse innebærer at man identifiserer forskjellige typer uønskede hendelser og derigjennom skaffer seg oversikt over hvilke utfordringer ulike situasjoner kan medføre innenfor det området man har ansvar for. Deretter er det viktig å finne hvilke tiltak som kan avhjelpe.
De hyppigste årsakene til tap av ekomforbindelse er:

- strømbrudd
- linjebrudd
- tekniske feil
- unormalt stor trafikk

4.1 Strømbrudd

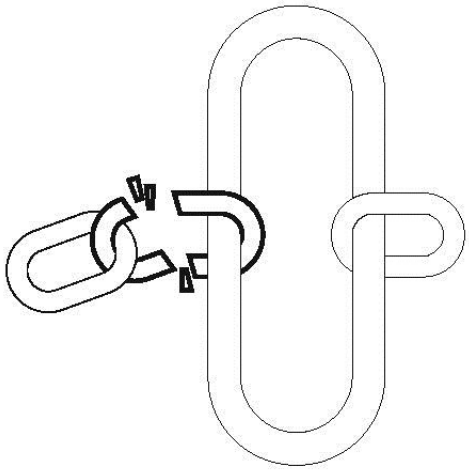
Alt ekomutstyr er avhengig av strøm. Utstyr i transportnettet og i kjernedelen av nettene er godt sikret mot strømbrudd. I tilgangsnettet kan varighet av reservestrøm variere fra null til noen få timer. Basestasjoner i mobilnettene har typisk mindre reservestrøm enn utstyr i fastnettet. Batterier sørger i de fleste tilfeller for at kortere strømbrudd ikke får noen konsekvenser for tjenestene. Når strømmen blir borte så lenge at batterier som leverer reservestrøm til utstyr i nettene, blir utladet, faller tjenestene ut.
Det kan være flere basestasjoner som dekker et bestemt område. Alle stasjonene faller ikke nødvendigvis ut samtidig. Men selv om en eller noen få basestasjoner sørger for fortsatt dekning, kan trafikk-kapasiteten disse har være for lav til å ta unna trafikkpåtrykket.
Tjenester basert på bredbånd er avhengig av lokal strøm ute hos abonnenten. Det stilles krav til reservestrøm for utstyr i nettene, men det hjelper ikke ved strømbrudd om utstyret i nettene er sikret med aggregater og batterier, hvis det ikke er strøm på utstyret ute hos abonnenten.



Figur 3: Når strømmen går, virker ikke brukerutstyret

4.2 Linjebrudd

En annen uønsket hendelse som kan medføre utfall av ekom, er linjebrudd i sambandsinfrastrukturen. Kabler kan bli revet over ved graveuhell eller jordras, kabler som henger på stolper kan bli tatt av trær som blåser over ende og master med antenner kan knekke under belastningen av is og sterk vind.
Tilgangsnettet kan være felles for flere tjenester og mangler oftest alternative linjer (redundans). Linjebrudd i denne delen av nettet kan i noen tilfeller føre til utfall av alle tjenester i et område.
Ett enkelt linjebrudd i transportnettet kan føre til utfall eller begrenset kapasitet for ekomtjenester i et avgrenset geografisk område. Flere samtidige linjebrudd kan føre til bortfall eller begrenset kapasitet for tjenester i større områder og noen ganger i hele landsdeler. I denne veilederen forfølger vi ikke muligheten for feil i transportnettet, siden det likevel ligger utenfor det den enkelte kommune kan sikre seg mot.



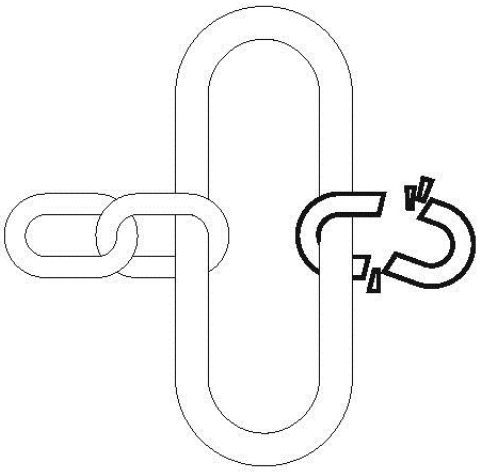
Figur 4: Tilgangsnettet kan rammes av linjebrudd

4.3 Tekniske feil

Det kan oppstå interne fysiske eller logiske feil i de ulike elementene som et ekomnett består av (nettverkselementer og programvare), og ikke bare feil som skyldes eksterne hendelser som uvær, flom og ras.

Fysiske feil er for eksempel overopphetning av komponenter som følge av svikt i kjøling, feilmontering og skader på komponenter under vedlikehold. Dette er feil som igjen kan føre til at et helt system slutter å fungere som forventet.

Logiske feil kan være feil i programvare som styrer trafikken eller produserer tjenester i ekomnett. Ett eksempel er feil i operativsystemet på en ruter som videresender datapakker, et annet er at systemer fra ulike leverandører er konfigurert på måter som ikke virker sammen. Etter som mer og mer av funksjonaliteten i nettene har med programvare å gjøre, vil logiske feil utgjøre en stadig større andel av feilårsaker. Denne type feil i kjernenettet vil kunne ha konsekvenser for mange brukere og store områder og i verste fall for hele tjenester i hele landet.



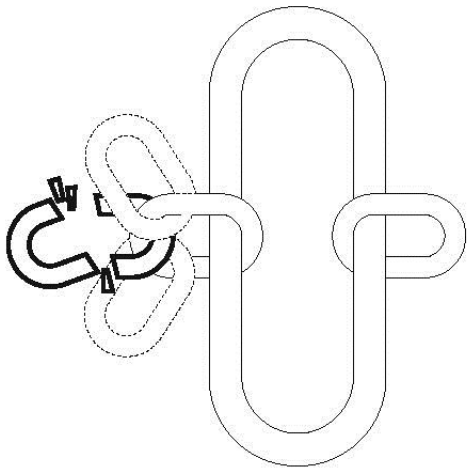
Figur 5: Logiske feil kan slå ut en hel tjeneste i kjernenettet

4.4 Unormalt stor trafikk

Mobilnettene er bygget ut med flere tusen basestasjoner som til sammen dekker det meste av landet. Fra sted til sted kan det likevel være stor variasjon i antall samtidige samtaler og mengden datatrafikk som nettet har kapasitet for. På steder hvor det normalt er få brukere vil det gjerne være langt mindre kapasitet enn i tettbygde strøk.

Hvis det skjer en ulykke på et sted med begrenset kapasitet i mobilnettene, kan det oppstå problemer med å bruke telefonen når redningsmannskap, skuelystne og journalister ringer og sender bilder osv. samtidig.

Store hendelser, for eksempel en konsert eller en festival, kan også bidra til at kapasiteten i mobilnettene settes under press, fordi mange vil dele store øyeblikk over nettet samtidig.



Figur 6: Ved store hendelser kan kapasiteten bli sprengt ved at for mange kjemper om en begrenset ressurs

Logiske feil, omtalt i avsnittet over, kan i noen tilfeller skyldes villede handlinger som hacking og terrorisme. I den primitive enden av skalaen for slike handlinger finner en tjenestenektangrep (DDoS[10]). Ved slike angrep sendes forstyrrende trafikk rettet mot visse IP-adresser, gjerne et sammenhengende spenn av adresser. Kommuner har tjenester som brukerne når via Internett. Over det samme nettet kan også hackere angripe disse tjenestene. Kommuner kan dermed rammes av tjenestenektangrep, dvs at deres servere bombarderes av trafikk fra nettet slik at de ikke blir i stand til å betjene reell trafikk.

4.5 Sårbarheter i dagens nett og tjenester

For å møte samfunnets avhengighet, bygges mye sikkerhet inn i selve ekominfrastrukturen. Alternative framføringsveier mellom punkter i nettet, dublering av utstyr, reservestrøm til det viktigste utstyret er typiske tiltak operatørene gjør for å sikre nettene sine. Slik sett blir infrastrukturen samlet sett mer robust. Noen egenskaper ved dagens nett kan likevel representere sårbarheter som er verd å merke seg. Med

[10] Distributed Denial of Service

sårbarheter menes her egenskaper som gjør nettene sårbare for truslene beskrevet i 4.1– 4.4. Disse kan oppsummeres til:

- Nye tjenester er ofte mer sårbare for strømbrudd lokalt enn tradisjonell fasttelefoni var. Telefonsentralene hadde reservestrøm i flere timer og telefonene var forsynt med strøm fra sentralen. Bredbånd og mobiltelefoni er avhengig av strøm lokalt for å virke.
- Tilgangsnettene har fortsatt i liten grad redundans. Dette vil si at mens det lenger inn i nettene er to og tre alternative veier mellom knutepunkter, slik at det er mindre kritisk om en av veiene ikke virker, er det annerledes ytterst i nettene, der den enkelte abonnent er knyttet opp – mobilt eller fast. Der er det ofte bare enkle linjer.
- Det er begrenset grad av lokal autonomi. Det tradisjonelle telefoninettet var bygget opp av lokale telefonsentraler som var knyttet sammen til et landsdekkende nett. Så lenge den lokale sentralen virket, kunne man ringe innenfor lokalområdet. I dag er mange ekomtjenester avhengige av at sentrale elementer i nettet fungerer og kan kommunisere med den enkelte bruker. Logiske feil i programvare kan for eksempel ramme kritiske funksjoner i en tilbyders kjernenett og dermed hele tjenesten.
- Mobilnettene er ikke dimensjonert for ekstreme lokale trafikktopper. Så lenge fastnettet var den viktigste infrastrukturen, var trafikktoppene mer forutsigbare og det var dermed enklere å dimensjonere nettene med riktig kapasitet. Det sier seg selv at når brukerne er mobile, er det umulig å dimensjonere kapasiteten i nettene slik at en tar høyde for alle tenkelige tilfeller. Derfor vil det kunne oppstå brist på kapasitet lokalt i mobilnettene ved uforutsette hendelser.

5 Praktiske råd

I moderne ekomnett er tilbudet av tjenester rikere enn i gamle nett. Nye tjenester som leveres over ekomnettene, kan være bedre tilpasset behovet enn gamle. Det er derfor ingen dyd å tviholde på gamle løsninger ut fra et beredskapshensyn, men det er viktig å ha et bevisst forhold til robustheten til de løsninger som velges.

Alle som har beredskapsansvar, og som er avhengig av ekom for å ivareta dette, bør kjenne til ulike løsninger for tilknytning til mobilnett, satellittnett og fastnett og hvordan man kan sikre strømforsyningen til eget utsyr. Med relativt enkle grep kan kommuner redusere risikoen for at ekomtjenestene de er avhengig av, blir utilgjengelige.

Med utgangspunkt i den enkle modellen av ekomnettene (figur 2) og truslene over (figurene 3-6), vil effektive tiltak være

a) lokale reserveløsninger for strøm
b) flere uavhengige forbindelser i tilgangsnettene
c) abonnement hos flere tilbydere med uavhengige kjernenett
d) prioritetsabonnement i mobilnett

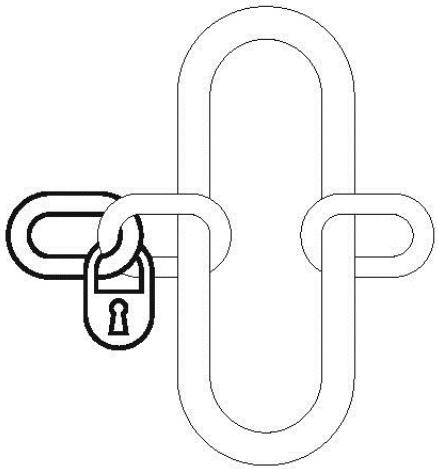
5.1 Ekstra strømforsyning til eget utstyr

En av de vanligste årsakene til at elektronisk kommunikasjon svikter, er mangel på strøm til utstyr som bidrar til produksjon av ekomtjenester. Det er tilbydernes ansvar å sørge for gode reserveløsninger for strøm i selve nettene, i tråd med myndighetspålagte krav. Men brukere må forholde seg til sårbarheten for strømbrudd hos seg selv. Mulighet for å bruke mobiltelefoner, modem, svitsjer, rutere, betalingsterminaler og datamaskiner, forutsetter tilgang til strøm. Kommuner er sårbare for konsekvensene av å være uten elektronisk kommunikasjon, og det er viktig at de sikrer utstyr, som de har ansvaret for selv, med reservestrøm. Eksempler på reservekilder for strøm er batterier, brenselceller, avbruddsfri strømforsyning[11] og aggregater.

Hvilken løsning som velges avhenger av kostnader og hvor sårbar man er for selv korte bortfall av strøm. Korte strømbrudd forårsaker ofte komponentfeil i elektronisk utstyr. Avbruddsfri strømforsyning fungerer som en buffer mot strømnettet og sikrer

[11] Vanlig engelsk betegnelse: Uninterruptible Power Supply - UPS

mot korte brudd og gir vern mot overspenning som kan forekomme for eksempel ved lynnedslag.

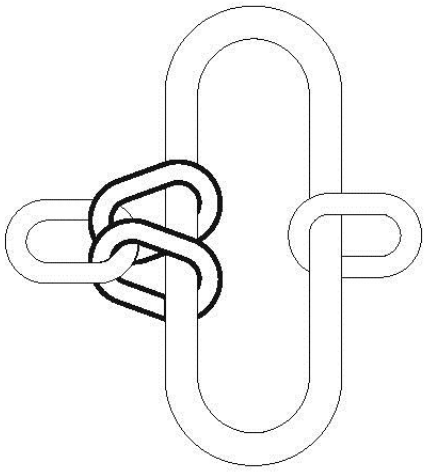


Figur 7: Ekstra strømforsyning reduserer sårbarheten lokalt

5.2 Flere uavhengige forbindelser

Det finnes over 200 tilbydere av elektroniske kommunikasjonsnett og elektroniske kommunikasjonstjenester i Norge. Mange av disse er lokale, for eksempel kraftselskaper, og har eget nett bare i et begrenset område. Hvis en bruker ønsker å redusere sårbarheten for linjebrudd, er det viktig å velge tilbydere som benytter ulike fysiske tilgangsnett. Dette vil redusere risiko for utfall, slik at selv om ett tilgangsnett ikke virker lokalt, er det mulig å benytte et annet fysisk tilgangsnett.

For taletjeneste vil et opplagt tiltak være å sørge for å ha både fasttelefon og mobiltelefon. Når det gjelder å beskytte seg mot faren for linjebrudd, kan fasttelefoniløsningen like gjerne være IP-basert som tradisjonell. Poenget her er at fasttelefonen i begge tilfeller har et annet tilgangsnett enn mobiltelefonen har.



Figur 8: Flere tilgangsnett reduserer sårbarheten for linjebrudd

5.2.1 Mobil datakommunikasjon

Alle mobilnettene som formidler tale, tilbyr også mobilt bredbånd i sine nett. ICE tilbyr ikke taletelefoni, men mobilt bredbånd. Det er mulig å benytte bredbåndstelefoni som kommuniserer over Internett for å ringe til det offentlige telefonnettet.

En teknisk forskjell mellom det mobilnettet ICE har i dag og de andre mobilnettene, er at ICE-nettet sender med lavere frekvenser. Dette medfører at signalet mellom basestasjon og telefon/modem når frem over lengre avstander. En basestasjon i ICE-nettet dekker typisk større områder enn basestasjoner i de andre mobilnettene. Ved et lokalt strømbrudd i området der brukeren befinner seg, er det dermed litt mer sannsynlig at det området der basestasjonen befinner seg, ikke er rammet enn det er for de andre mobilnettene. I så fall kan brukeren fortsatt benytte kommunikasjonstjenestene så lenge utstyret har strøm via batteri eller alternativ strømkilde. Tilgjengelig båndbredde vil imidlertid reduseres med mange brukere og lang avstand til basestasjonen.

5.2.2 Bredbånd

Fast bredbånd leveres de fleste steder over både fiber- og kobberkabler. Selv om en kommune har sin hovedforbindelse for bredbånd på fiber, kan det være en rimelig forholdsregel å beholde eller eventuelt nytegne et DSL-abonnement som reserve.

Denne forbindelsen kan ha lavere kapasitet, men likevel være tilstrekkelig til prioriterte formål. For at dette skal være en reell sikring mot for eksempel overgraving, må en forsikre seg om at fiber- og kobberkabel ikke går i samme grøft.

5.2.3 Faste samband

En kommune har ofte ansvar for en intern IT- og kommunikasjonsinfrastruktur og kjøper eller leier samband mellom punkter i denne infrastrukturen. Slike samband må også tas med i en helhetlig ROS, og det vil ofte være nødvendig å ha reserveløsninger for slike punkt-til-punktsamband. Ved bruk av kabel eller radiolinje, kan en ekstra fremføringsvei til bygningen eller virksomheten bidra til redusert sannsynlighet for utfall av elektroniske kommunikasjonstjenester. Avhengig av hvor mye kommunen velger å drifte selv og hvor mye den velger å kjøpe av tilpassede tjenester, kan alt fra kabelpar (for eksempel mørk fiber) til samband med spesifisert ytelse og såkalt spredt ruting, være aktuelt. Spredt ruting vil si at to samband mellom tilknytningspunkter i transportnettet, legges på forskjellige nettressurser.

Det kan være ulike teknologier som benyttes for fremføring til brukeren. Det viktigste er imidlertid at disse fremføringene er uavhengige av hverandre slik at ikke eksempelvis to kabler ligger i samme grøft og et graveuhell kan føre til brudd i begge kablene samtidig. Kombinasjonen av kabel og radiolinje kan være et alternativ til separate fremføringsveier for kabler inn til bygningen eller virksomheten. Jo lenger inn i nettet man kan sikre virkelig alternative fremføringsveier, jo bedre er man sikret mot et enkeltbrudd.

Det er et tilsynelatende paradoks her som er verd å merke seg: Man kan være sikrere på å oppnå reell redundants for samband mellom to punkter ved å bestille disse hos én tilbyder enn ved å kjøpe linjer hos flere uavhengige tilbydere. I det siste tilfellet har man mindre sikkerhet for at forbindelser som er uavhengige på bestillingspunktet, over tid kan havne i samme føringsvei eller bli avhengig av felles ressurser.

5.3 Flere uavhengige abonnement

5.3.1 Mobilabonnement

Det er flere fysiske mobilnett i Norge. Derfor er det et enkelt og rimelig tiltak at alle som har beredskapsansvar, har abonnement hos minst to mobiltilbydere: Ett som man bruker til daglig, og ett i reserve hvis hovedabonnementet ikke skulle virke. Det er da viktig å velge tilbydere som benytter seg av ulike mobilnett. Et slikt tiltak reduserer

virksomhetens sårbarhet for tekniske feil i kjernenett så vel som for linjebrudd i tilgangsnett.
Noen av tiltakene i kapitlet over, som sikrer flere forbindelser, gir altså samtidig større robusthet overfor feil i kjernenettet. Et eksempel på det er mobilabonnement hos TeliaSonera og Telenor. Hos disse er både tilgangsnett og kjernenett adskilte. I andre tilfeller kan tjenester kun være skilt i kjernenettet, for eksempel mobiltelefoni fra Telenor og Ventelo.

Det er viktig å bruke det ekstra abonnementet iblant, slik at det ikke blir inaktivt, og det er lurt å gjøre nummeret tilgjengelig for dem som trenger å komme gjennom når hovednummeret ikke virker. En praktisk måte å håndtere et slikt ekstra abonnement på, er å kjøpe et billig abonnement eller et kontantkort og installere det i en telefon man ikke bruker til daglig, og deretter sende en sms eller ta en kort samtale iblant, slik at man sjekker at alt virker og at telefonen er oppdatert. Noen mobiltelefoner har også muligheten for å ha to SIM-kort installert samtidig, noe som forenkler bruken siden en ikke behøver å sette inn det ekstra SIM-kortet ved skifte til en annen tilbyders nett.

5.3.2 Bredbåndsabonnement

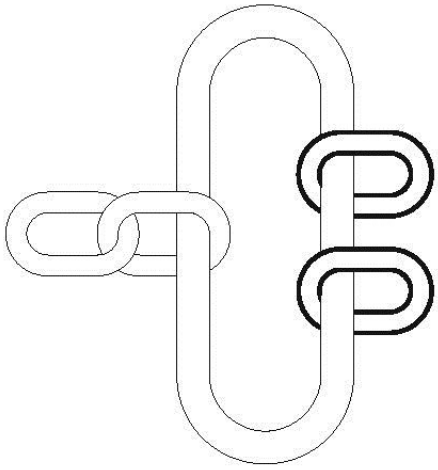
Under punkt 5.2.2 påpekte vi at ulike bredbåndsabonnement kan redusere sårbarheten for linjebrudd. Ved å sørge for at abonnementene er hos to forskjellige Internett-tilbydere (Internet Service Provider - ISP), vil en i tillegg være bedre rustet mot feil i kjernenettene.

I en kommune er ikke bare sentraladministrasjonen, men også institusjoner som skoler og biblioteker tilknyttet Internett. De siste er mye mer typiske mål for tjenestenektangrep enn administrasjonen siden noen oftere deltar i spill fra slike steder. Et tiltak for å beskytte administrasjonen for tjenestenektangrep, kan være å ha separate Internett-tilknytninger for elevnett på skoler. Beskyttelsen er størst om tilknytningene er hos ulike ISP-er siden en da er sikrest på at tilknytningene har adressemessig god avstand.

5.3.3 Andre tjenester

Selv om IP-telefoni og tradisjonell fasttelefoni begge kan leveres over samme fastlinje i tilgangsnettet, produseres tjenestene uavhengig av hverandre i kjernenettet. Å ha begge typer abonnement vil redusere sårbarheten for å miste fasttelefoni helt ved en teknisk feil.

I mange tilfeller settes drift av applikasjoner ut til eksterne leverandører. Når de eksterne leverandørene tilbyr slik drift i storskala datasentre på Internett, omtales det gjerne som skytjenester. E-post regnes vanligvis ikke som en ekomtjeneste, men det er uansett en viktig tjeneste for en kommune. Derfor bør en sikre tilgjengelighet for den på tilsvarende måte som for ekomtjenester. For tilgjengelighet alene, kunne skybasert e-postleveranse hatt attraktive egenskaper for en kommune. Her vil det først og fremst være andre hensyn, særlig krav til konfidensialitet, som taler i mot en slik løsning. Best robusthet oppnår en hvis en har redundante servere for e-post plassert på geografisk adskilte steder og gjerne i ulike operatørers IP-nett. Servere som speiler hverandre reduserer sårbarheten for enkeltfeil og gir større motstandsdyktighet mot tjenestenektangrep.



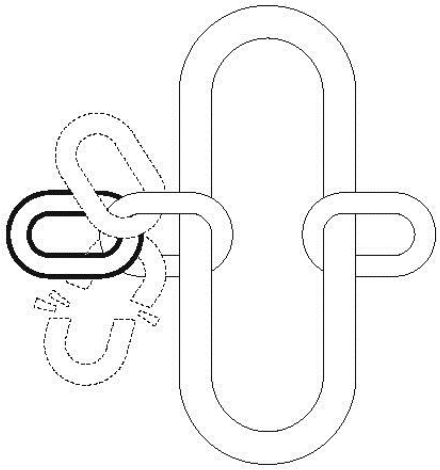
Figur 9: Ved å abonnere på uavhengige tjenester, vil en ikke så lett bli slått ut av feil i kjernenettet

5.4 Prioritet i mobilnett

Mobiltilbydere i Norge tilbyr prioritetsabonnement. Ordningen for prioritet i mobilnett er opprettet for å øke muligheten for å komme gjennom med taletrafikk i mobilnettene, selv når en hendelse har gjort at det er overbelastning eller svært begrenset kapasitet i nettet. Et prioritert anrop vil kunne bryte andre samtaler når det er knapt om radiokanaler i tilgangsnettet og man vil dessuten ha nasjonal gjesting. Nasjonal

gjesting vil si at hvis det mobilnettet der en er abonnent, lokalt faller bort eller mangler dekning, blir trafikken formidlet gjennom et av de andre nettene. På samme måte som ved internasjonal gjesting, er en avhengig av at gjestenettet er i stand til å kontakte ens hjemmenett. Prioritetsordningen er dimensjonert for inntil 10 000 brukere.

Ordningen for prioritet i mobilnett er opprettet for å ivareta brukere som har ansvar for kritiske funksjoner i samfunnet og kommuner er kandidater for ordningen. Begrensningen på antall brukere i ordningen innebærer at den enkelte kommune eller virksomhet først og fremst må sørge for at nøkkelpersoner innenfor krise og beredskap tilgodeses med slike abonnement. Merk i den sammenheng at ordningen først og fremst er til hjelp for de som har behov for å ringe ut. Virksomheter (for eksempel en kommune) skal søke PT om godkjenning via Altinn før de kan tegne abonnement. Tilbydere vil normalt kreve at prioritet knyttes til bedriftsabonnement. Se PTs hjemmeside npt.no for mer informasjon om hvordan skaffe prioritetsabonnement. Relevant informasjon kommer opp ved å søke på nøkkelordet «prioritet».



Figur 10: Med prioritetsabonnement oppnår en å komme gjennom selv når nettet er fullt – om nødvendig på bekostning av uprioritert trafikk

5.5 Satellittkommunikasjon

Kommunikasjon via satellitt vil ikke påvirkes av linjebrudd eller utfall av elektrisk kraft i eget nærområde, så lenge brukeren har sikret strømtilførsel til sin egen satellittelefon. Slik sett er satellittkommunikasjon et alternativ som reduserer ens sårbarhet for totalt bortfall av ekomtjenester. Kapasiteten er mye lavere enn i bakkebaserte nett og derfor har dette alternativet større relevans som kriseløsning (se 6.4) enn for det generelle behovet for robuste ekomløsninger.

5.6 Trygghetsalarmer

Kommuner har mange brukere av trygghetsalarmer. I ulik grad kan kommuner ha påtatt seg ansvar for slike løsninger. Leverandør av ekomtjenesten hvor alarmene overføres og leverandør av selve trygghetsalarmen er gjerne ikke de samme. Det kan gjøre drift av slike løsninger ekstra utfordrende. Trygghetsalarmer kan benytte ulike overføringsteknologier som fasttelefon, GSM eller IP. Man bør unngå å binde seg til løsninger som bygger på teknologi som fases ut og helst velge løsninger som kan kommunisere over flere tilgangsnett. Det er viktig å være klar over hvilke ekomtjenester de aktuelle løsningene er avhengig av. Ved en overgang fra for eksempel analog telefonlinje til IP-basert kommunikasjon, må man huske at den siste er avhengig av lokal strøm.

5.7 Avtal tjenestekvalitet med tilbyder

Det er viktig å diskutere kvalitet og sikkerhet med den eller de tilbyderne som er valgt for leveranse av elektroniske kommunikasjonstjenester. En slik avtale betegnes ofte som en SLA-avtale (Service Level Agreement). En avtale om leveransekvaliteten bidrar til en felles forståelse av hva som kan forventes av utilgjengelighet i en spesifisert tidsperiode. Det kan være aktuelt å avtale spesifikke krav til maksimal rettetid, slik at det er mulig å vite hvor lenge et driftsavbrudd kan forventes å vare. Økonomisk kompensasjon ved brudd på rettetids- eller tilgjengelighetskrav bør også avtales. Videre bør avtalen inneholde spesifikk informasjon om hvordan tilgjengelighet sikres gjennom bruk av alternative fremføringsveier og hvilken reservestrømskapasitet tilbyder har tilgjengelig i tilgangsnettet der hvor en knyttes til.

Post- og teletilsynet har utarbeidet en mal for SLA[12] som kan finnes på Nettvett.no. En god SLA-mal kan også gjøre nytte som sjekkliste der hvor partene velger en annen måte å dokumentere kontraktsforholdet på.

Det er vanskelig og dyrt å sikre seg godt mot tjenestenektangrep fra Internett. Det viktigste en kommune kan gjøre på forhånd, er å avgjøre hvilke tjenester som er viktigst å beskytte og kommunisere dette til sin ISP. På den måten vil ISPen være i stand til å gi best hjelp når det gjelder. Nasjonal Sikkerhetsmyndighet (NSM) har gitt ut en publikasjon[13] hvor de gir veiledning om noen grunnleggende tiltak for sikring av IT-systemer mot tjenestenekt-angrep.

[12] Utarbeidet i samarbeid med IKT Norge (tidligere NORTIB)
[13] https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/u-04_ddos_v1.0.2.pdf

6 Ekom i krisesituasjoner

I planlegging av kriseberedskap må en kommune se nøye på de forskjellige typer kommunikasjon den har behov for, og hvilke løsninger som er hensiktsmessig å bruke for å møte behovene. En ROS kan avdekke utfordringer, identifisere tiltak som er nødvendig å iverksette, og samarbeidsrelasjoner som bør bygges før en krise inntreffer, slik at kommunikasjon kan sikres.

DSB har gitt ut en veileder i risiko- og krisekommunikasjon[14] som særlig legger vekt på kommunikasjon ut mot befolkningen. PTs mål med dette kapitlet er å formidle praktiske råd til bruk av ekom i håndtering av en krise som rammer en kommune og tilgangen til de vanlige ekomtjenestene er borte eller sterkt redusert.

6.1 Beredskapsplaner

I beredskapsplanleggingen er det viktig å ta høyde for at enkelte scenarier innebærer at flere uønskede hendelser oppstår samtidig. Dersom skred eller uvær fører til linjebrudd i elektroniske kommunikasjonsnett, er det risiko for at dette skjer samtidig med strømbrudd. Da kan det ha stor betydning for utfallenes varighet at arbeidet med å reparere skadene skjer på en koordinert måte, og at forskjellige feil rettes i riktig rekkefølge. Veier må ryddes slik at feltmannskap kommer fram, og skader på strømnett kan medføre at et skadested må sikres før mannskap som reparerer linjebrudd i elektroniske kommunikasjonsnett får slippe til. God planlegging er derfor essensielt for å minimere tidstapet i en krevende situasjon.

6.1.1 Behov for utstyr

Beredskapsplanlegging bør omfatte kartlegging av kommunikasjonsbehov og hva slags utstyr det kan være behov for i en krisesituasjon. Dette utelukker ikke at det i en faktisk krisesituasjon må improviseres andre løsninger, men et viktig formål med planer og kartlegging er å sikre at det blir anskaffet et minimum av beredskapsmateriell og at det blir gitt opplæring i hvordan dette utstyret skal brukes.

Kartlegging av tilgjengelig utstyr vil avdekke hva slags utstyr som er tilgjengelig, enten det er eid av offentlige etater eller det kan gjøres avtaler om at utstyret kan rekvireres etter behov. Når dette er gjennomført, vil behovet for å anskaffe ytterligere beredskapsmateriell avdekkes.

[14] http://www.dsbinfo.no/DSBno/2014/Tema/risikoogkrisekommunikasjon/

6.1.2 Samspill mellom utstyr

I enkelte situasjoner kan flere typer infrastruktur være skadet og reparasjonsarbeidet må koordineres for å gjenopprette viktige tjenester så raskt som mulig. Ekom er som regel en viktig ressurs for å koordinere og gjennomføre de forskjellige reparasjonene på en trygg og effektiv måte. Noen sektorer har tilstrekkelig utstyr for å gjennomføre sin egen del av arbeidet, men har ikke nødvendigvis utstyr som lett kan «snakke» med andre sektorers utstyr. Det er viktig å tilrettelegge for koordinering slik at man disponerer det utstyr og de ressurser som er nødvendige for at kriseledelsen kan koordinere.

6.1.3 Opplæring og øving

Gode planer og forhåndsanskaffelse av reserveutstyr for en krise kan vise seg å ha liten verdi dersom planene ikke er tilstrekkelig kjent og ingen er fortrolig med å bruke utstyret. Opplæring og øving er derfor en nøkkel til å lykkes. Det er viktig å gjennomføre øvelser regelmessig, og da med deltagere fra de forskjellige etater og virksomheter slik at en vet at utstyr og systemer kan fungere sammen.

6.2 Kontaktinformasjon

Det er nyttig å lage telefonlister med alternative telefonnummer som kan brukes i situasjoner med delvis utfall i elektronisk kommunikasjon. Disse listene må være distribuert som en del av kriseplanene, og det kan være hensiktsmessig å gjennomføre regelmessige kommunikasjonsøvelser for å sjekke at telefonlistene er riktige. Listene bør også skrives ut på papir og ligge hjemme hos dem som har ansvaret, pluss i bil eller fritidsbolig. Korte tekstmeldinger kan benyttes som alternativ til talebeskjeder, men det krever etablerte rutiner for å bekrefte at meldingene er mottatt av alle som skal ha dem.

De fleste har privat e-post uavhengig av jobbens e-post. Privat e-post er ofte levert som skytjenester. I en krise kan dette representere en alternativ mulighet for å kommunisere. En kommune kan også selv opprette slike ekstra e-postkontoer for sine ansatte. Selv om slike tjenester ikke skulle oppfylle kommunens normale krav til sikkerhet, vil de kunne være et alternativ når tilgjengelig er det overordnede kravet. I alle tilfeller må adresseinformasjonen være dokumentert og tilgjengelig for å kunne benyttes i en krisesituasjon.

6.3 Lokalt samband

Noen ganger kan alle offentlige nett være nede. For lokal talekommunikasjon kan VHF-radio være et alternativ til fast-, mobil- og satellittelefon. Hvis behovet er stort, kan man anskaffe VHF-radioer som beredskapsutstyr, og i noen kommuner finnes sikringsradioer og jaktradioer som kan inngå i en lokal beredskapsplan der de lokale forholdene tilsier det. Det er viktig at det gjøres avtaler på forhånd, og at personell som skal bruke utstyret, øver regelmessig. Det er også viktig å få oversikt over dekningsområdet for denne typen samband, slik at begrensninger utstyret har med hensyn til rekkevidde osv. er kartlagt.

6.4 Satellittkommunikasjon

Det finnes flere satellittbaserte telefonitjenester, og med noen av disse kan man også sende tekstmeldinger og e-post, og ha generell tilknytning til Internett.

Satellittkommunikasjon er avhengig av at det er fri sikt mellom satellitten og telefonen. I enkelte dalfører kan det være områder som ligger i satellittskygge. Satellittelefoner kan stort sett ikke benyttes innendørs, fordi radiosignalene er for svake. Det er dermed nødvendig å få montert utvendig antenne i lokaler hvor det er behov for å benytte satellittelefon, eller ha en løs antenne. Håndholdte satellittelefoner er i dag å få kjøpt relativt rimelig, og som mobiltelefoner får de plass i en lomme og kan bringes med etter behov. De fleste satellittelefoner er batteridrevne, og har begrenset brukstid før de må lades.

Noen systemer baserer seg på lavbanesatellitter og andre på geostasjonære. Hvilket system som egner seg best og er mest kostnadseffektivt, vil variere fra sted til sted. I noen kommuner kan det være hensiktsmessig å basere seg på begge typer system.

Noen telefoner for systemet Globalstar kan også ta SIM-kort slik at den samme telefonen også kan brukes mot et GSM-nett. I de regionene hvor Globalstar har samtrafikkavtale med lokale mobilnett-operatører vil det være mulig å bruke samme telefonnummer både ved bruk av GSM-nett og satellittnett. En annen tilbyder er Thuraya, og deres håndholdte terminaler kan også kommunisere gjennom GSM-nettet i tillegg til via satellittnettet. Inmarsatsystemet har håndsett for tale og i tillegg tilbyr de bærbare enheter for datakommunikasjon.

Det finnes relativt enkle og rimelige løsninger hvor en kappe med batteri og satellittdelen kan settes bakpå en vanlig iPhone eller Android-type smarttelefon slik at telefonen kan brukes som normalt og et program (app) på telefonen aktiverer satellittdelen. Dette gjør det enkelt for brukeren å skifte fra normal mobiltrafikk til satellittrafikk. Det finnes også små satellittenheter i handelen for å sende og motta SMS og e-post.

Breiband.no tilbyr bredbånd via Eutelsats geostasjonære satellitter. PT kjenner ikke til hvor brukbar en eventuell telefonitjeneste (for eksempel Skype) over en slik bredbåndsforbindelse vil være. Det er grunn til å forvente at talekvaliteten vil være bedre på tjenester som tilbys spesielt for tale (ref. Inmarsat og Thuraya).

For faste punkt med tilgang på strøm vil det beste alternativet være en to-veis satellittforbindelse gjennom en fastmontert parabolantenne. Slike løsninger har kapasitet på mange megabits per sekund.

6.5 Kommunikasjon med andre etater og sentrale myndigheter

Det må påregnes at det i en krisesituasjon er begrenset kapasitet i de offentlige nettene, men det bør i mange situasjoner være mulig å utveksle e-post og kommunisere via krisestøtteverktøy eller gradert samband. Det er viktig at det er etablert rutiner for slik kommunikasjon på forhånd. De fleste kommuner bruker krisestøtteverktøyet CIM, som er web-basert og ofte kun tilgjengelig over Internett. Selv om en kommune også må ha rutiner som ikke forutsetter tilgjengelige it-verktøy, er det viktig at tilgang til et slikt verktøy sikres så godt som mulig. Enkelte satellittelefoner (se over) kan brukes til å få tilgang til Internett i tillegg til ordinært talesamband.

Det kan, som vi har sett, være hensiktsmessig å ha abonnement hos flere alternative tilbydere som leverer tjenester over fysisk forskjellig infrastruktur. Dette gjelder i høy grad også når kriser skal håndteres. I en krisesituasjon kan man bruke smartmobilen til e-post, oppdatere nettsider og andre formål som har begrensede krav til overføringskapasitet. Det er derfor viktig at de som har ansvar for å betjene disse tjenestene til daglig, har lært seg å bruke dem via mobilen.

6.6 Nødnett

Nødnett, som skal stå ferdig i 2015, er et eget mobilnett som eies av Justisdepartementet og drives av Direktoratet for nødkommunikasjon (dnK). Det er i hovedsak beregnet på nødetatene (politi, helse og brann). For å kommunisere i dette nettet må en ha egne radiohåndsett for Nødnett.
Nettet tilbyr tale og enkel datakommunikasjon og har talefunksjoner som er tilpasset kommunikasjonsbehovet til beredskapspersonell. Eksempler på funksjoner er talegrupper, sikring mot avlytting, og «walkie-talkie»-type kommunikasjon. Nødnett har en infrastruktur som langt på vei er uavhengig av annen ekom.

Merk at Nødnett har ingen ting å gjøre med befolkningens mulighet for å ringe nødnumrene 110, 112 og 113. Anrop til nødnummere skjer via de vanlige fast- og mobilnettene.

Det er åpnet for at også virksomheter ut over nødetatene med et beredskapsbehov skal kunne søke om å bli brukere av Nødnett. Nødetatene har egne bemannede kommunikasjonssentraler som en del av sine løsninger, men for enkeltkommuner skal det være mulig å bli brukere uten å ha egen kommunikasjonssentral. Det kan i stedet være aktuelt å knytte seg opp mot sentraler for brann eller helse for å utnytte felles ressurser. Kommuner vil måtte betale for egne nødtelefoner i tillegg til en abonnementsavgift. For nærmere informasjon se hjemmesiden til dNk[15]. Tilgang til Nødnett kan være nyttig for å samhandle med andre aktører som for eksempel fylkesmenn.

6.7 Informasjon til befolkningen

Dersom en uønsket hendelse rammer elektroniske kommunikasjonstjenester, er det viktig å ha rutiner for hvordan man kan formidle viktige beskjeder til befolkningen. Der hvor Internett er tilgjengelig, vil en kommunes hjemmesider og sosiale medier være viktige kanaler for dette. De vanlige kanalene kan imidlertid være utilgjengelige og en kommunes beredskapsplan bør også omfatte alternative løsninger for å nå ut med informasjon til befolkningen. Hva slags løsninger som er praktisk gjennomførbare, vil avhenge av lokale forhold. Ofte vil mediene være en god samarbeidspartner for å gi råd til befolkningen og sikre distribusjon av viktig informasjon. En egen

[15] http://www.dinkom.no/

informasjonsplan for kriser, der tiltak ved bortfall i elektronisk kommunikasjon er ett punkt, er derfor å anbefale.

Elektronisk kommunikasjon omfatter også kringkasting. Dette er en viktig kanal for å formidle informasjon til befolkningen, særlig i situasjoner hvor det ikke er mulig å formidle slik informasjon gjennom Internett.

Regjeringen har opprettet et eget nettsted for kriseinformasjon til befolkningen. Ved hendelser av et visst omfang, vil Kriseinfo.no videreformidle informasjon til befolkningen, selv om ikke hele landet er rammet. Under brannene i Midt-Norge vinteren 2014, var kriseinfo en viktig informasjonskanal.