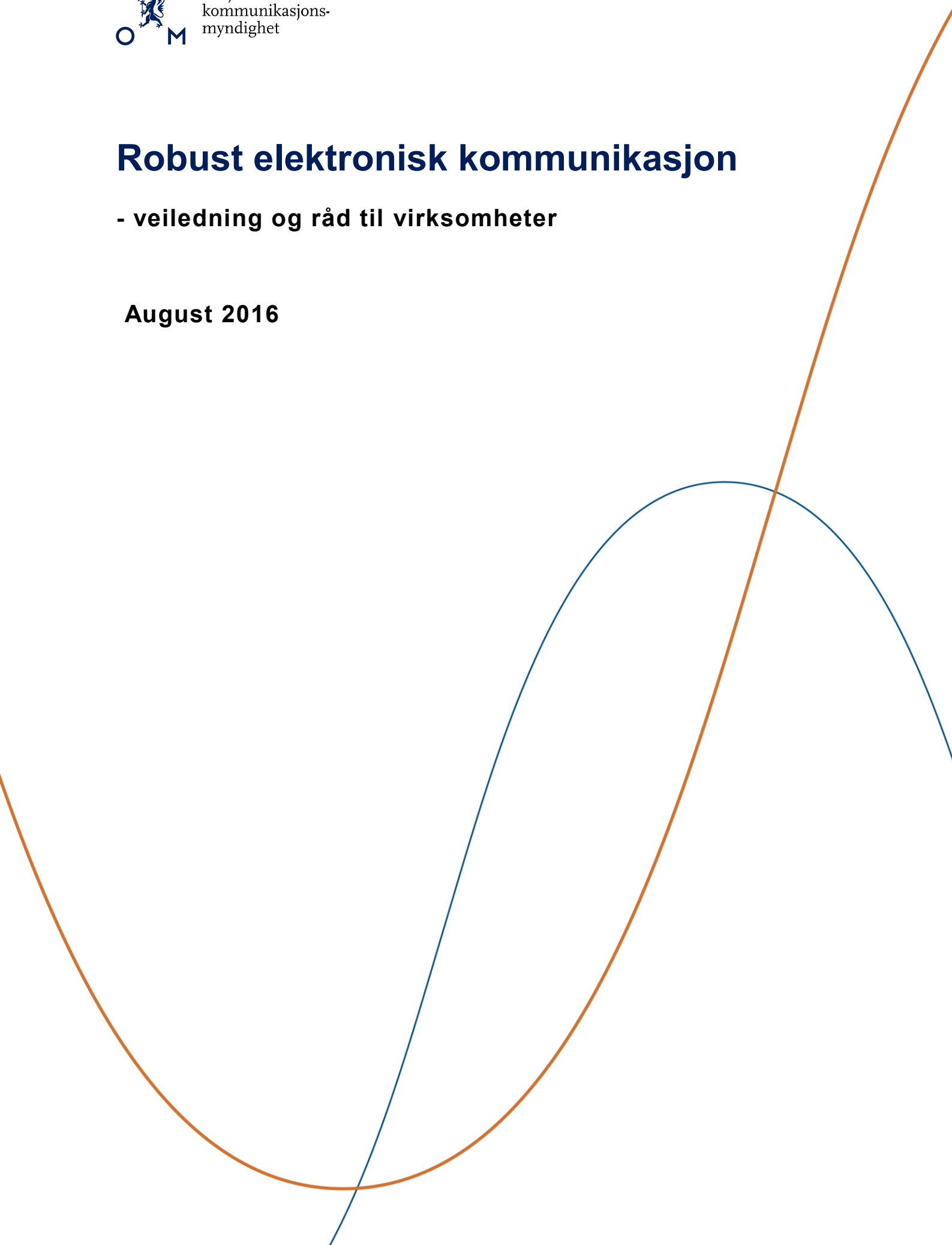
Nasjonal kommunikasjons-myndighet

Robust elektronisk kommunikasjon

- veiledning og råd til virksomheter

August 2016



Innholdsfortegnelse

1 Innledning

Offentlige virksomheter og private virksomheter som har viktige samfunnsfunksjoner forventes å utarbeide og vedlikeholde krise- og beredskapsplaner for å håndtere uønskede hendelser som kan ramme virksomheten. For noen typer virksomheter er dette regulert gjennom lov og forskrift. Gjennomføring av risiko- og sårbarhetsanalyser (ROS) inngår gjerne som en del av dette arbeidet.

De aller fleste funksjoner som en virksomhet utfører forutsetter at elektronisk kommunikasjonsnett og elektroniske kommunikasjonstjenester er tilgjengelig. Det er derfor svært viktig at virksomhetens bruk av elektronisk kommunikasjon (ekom) inngår i ROS-analysene og at avhengigheten gjenspeiles i krise- og beredskapsplanene.

For å lykkes med å skape et trygt og robust samfunn, er det avgjørende at alle tar ansvar for å sikre liv, helse, grunnleggende behov og verdier i forbindelse med hendelser og kriser.

2 Om veilederen

Målgruppen for veilederen er offentlige og private virksomheter, inkludert kommuner, som har en viktig samfunnsfunksjon. Nkoms mål med veilederen er å hjelpe virksomheter med å *redusere sannsynligheten for utfall av ekomnett og -tjenester,* ved å gjøre informerte valg ved anskaffelse av ekomtjenester og i valg av beredskapsløsninger. For kommuner finnes en versjon av veilederen som inneholder noe informasjon som gjelder særskilt for disse.

Veilederen avgrenser seg til råd som gjelder bruk av de offentlige ekomnettene, som mobil- og bredbåndsnett. I forbindelse med kravstilling ved innkjøp av ekomtjenester er enkelte tekniske aspekter ved robusthet i ekomnett beskrevet. Avhengig av virksomhetenes størrelse, vil man ha personell med teknisk kompetanse til kravstilling ved innkjøp av ekomtjenester. Denne veilederen er primært ment for de som har begrenset kompetanse på ekomområdet, men det er også tatt med råd og veiledning som gjelder større virksomheter, som for eksempel ved utsetting av tjenester til utlandet.

Veilederen legger størst vekt på *tilgjengelighet* av ekom. Andre sikkerhetsaspekter 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. Når det gjelder sikkerhet knyttet til behandling av personopplysninger, viser vi til Datatilsynets regelverk og veiledere.

Kapittel 3 handler om viktigheten av å involvere ekom som en del av virksomhetens helhetlige ROS-arbeid.

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 4 gir derfor en kort innføring i ulike ekomnett og tjenester.

Kapittel 5 handler om de vanligste årsakene til bortfall av ekomtjenester, mens kapittel 6 inneholder praktiske råd for valg av robuste ekomløsninger. Til slutt er Nkoms råd for å forberede seg på kommunikasjonsbehovet i krisesituasjoner samlet i kapittel 7.

3 Samfunnsikkerhet, ekom og ROS

Samfunnssikkerhet er definert som samfunnets evne til å opprettholde vitale samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenning, jf. Stortingsmelding nr. 17 (2001-2002). «Samfunnssikkerhet – veien til et mindre sårbart samfunn». Med dette utgangspunktet innebærer arbeidet med samfunnssikkerhet både forebygging, beredskap, krisehåndtering og gjenoppretting.

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.

Private og offentlige virksomheter har ansvaret for viktige tjenester til befolkningen. Kommunene har i tillegg ansvar 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, spesielt når kriser inntreffer.

ROS utføres på ulike nivåer og for ulike virksomheter. Innen enkelte områder er det er det krav til ROS i lov eller forskrift. Dette gjelder både for statsforvaltningen, og for regionale og lokale myndigheter som Fylkesmannen og kommunene. Det samme gjelder for mange private virksomheter som forvalter kritisk infrastruktur eller utfører viktige samfunnsfunksjoner.

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*[1]. DSB har utarbeidet en veileder[2] i

[1] Samfunnets sårbarhet overfor bortfall av elektronisk kommunikasjon (DSB 2012)

helhetlig risiko- og sårbarhetsanalyse for kommuner der sårbarhet overfor bortfall av ekomtjenester er en viktig del.

Norsk Standard 5814:2008 er en generell standard rettet mot fag, bransjer og næringer som ikke har egne standarder for risikovurdering. Standarden gir en beskrivelse av risikovurderingens plass i risikostyring og av faktorer som påvirker planlegging og gjennomføring av risikovurderinger, for eksempel rammebetingelser og etablering av risikoakseptkriterier. NS 5814:2008 kan være et utgangspunkt som mal for virksomheters ROS.

Når virksomheter gjennomfører en ROS som involverer ekom, må det avgjøres hvilken risiko som kan aksepteres når det gjelder utfall av ekom. Hvor mange minutter, timer eller dager kan de berørte 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 utfall inntreffer, og
2. de som reduserer *konsekvensene* når 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. Man må derfor ta forholdsregler også for å redusere konsekvensene hvis dette skulle skje. Tiltak i den siste kategorien kan omfatte manuelle rutiner og alternative kommunikasjonsløsninger.

[2] http://www.dsb.no/no/Ansvarsomrader/Regional-og-kommunal-beredskap/Aktuelt-Regional-og-kommunal-beredskap/veileder-for-ROS-analyse-i-kommunen/

4 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.

4.1 Ekomnett

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

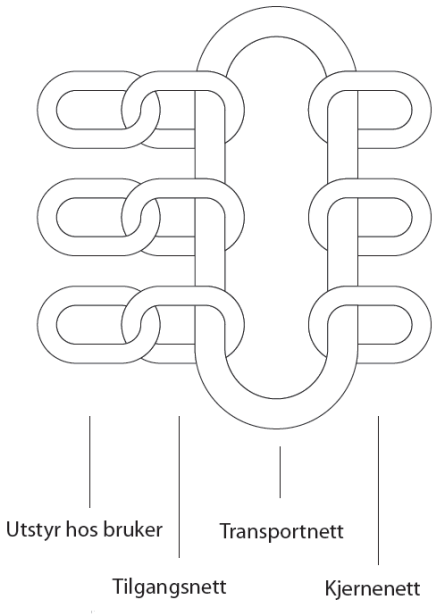
- Tilgangsnettet
  Tilgangsnettet er den delen av nettet som brukeren er tilknyttet. I mobilnettene er det basestasjoner som utgjør tilgangsnettet, for fast telefoni og bredbånd er det de lokale fiber- eller kobberkablene foruten utstyr i endesentraler. Imidlertid har nettene ofte ingen eller få alternative 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.

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

[3] Ofte kalt «backhaul» i fagterminologi

bruker på venstre side med ekomtjenester på høyre side. De tre nettkategoriene 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 1: 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, Telia, 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 Telia eller TDC 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.

4.2 Fastnett

I fastnettet er brukeren koplet til med kabel eller via radiolinje. Kabelen eller radiolinjen går fra 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

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

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 kobber- og fibernettet 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.

Hvis virksomheten har flere lokasjoner som skal knyttes sammen 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.

4.3 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 tre offentlige mobilnett i Norge, nettene til Telenor, Telia og ICE. Alle leverer både kombinerte abonnement for telefoni og datatjenester og særskilte bredbåndsabonnement. Telenor og Telia har landsdekkende nett. ICE har eget landsdekkende nett for mobilt bredbånd og jobber med å bygge opp eget 4G-nett også med telefonitjeneste. Der ICE selv ikke har dekning for telefonitjenesten benyttes Telias nett (gjesting). 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. De fleste tilbydere er rene tjenestetilbydere uten egen infrastruktur. Enkelte tilbydere kalles *virtuelle*[5] siden de kombinerer leid kapasitet med eget utstyr og tjenester.

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.

[5] Mobil virtuell nettverksoperatør (MVNO) (eng: Mobile Virtual Network Operator)

4.4 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 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.

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 Iridium og Globalstar 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

[6] http://www.inmarsat.com/
[7] http://www.thuraya.com/
[8] https://www.iridium.com/default.aspx

samtaler. Iridium er basert på 90-talls teknologi og har sammenlignbare ytelser med GSM, men de har annonsert en videreutvikling med høyere hastigheter.

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 systemet i større grad er avhengig av infrastruktur på bakken. I både geostasjonære- og lavbane satellittsystemer må signalene gå via en jordstasjon før det rutes videre i det offentlige telenettet eller Internett.

5 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.

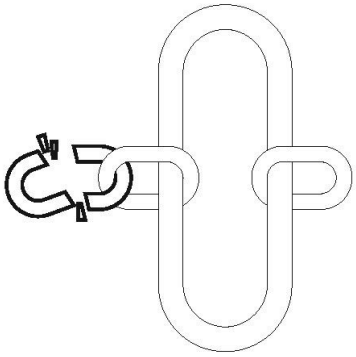
De hyppigste årsakene til tap av ekomforbindelse er:

- strømbrudd
- linjebrudd
- tekniske feil
- unormalt stor trafikk

5.1 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.
Flere basestasjoner kan dekke et bestemt område. Alle stasjonene faller ikke nødvendigvis ut samtidig. Selv om en eller noen få basestasjoner sørger for fortsatt dekning, kan trafikkapasiteten 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 ved strømbrudd hjelper det ikke om utstyret i nettene er sikret med aggregater og batterier, hvis det ikke er strøm på utstyret ute hos abonnenten.

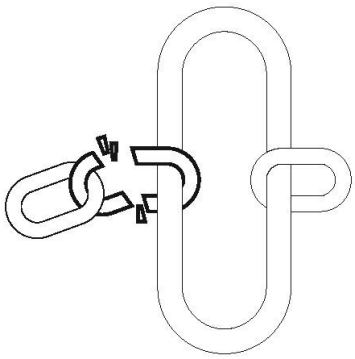
[9] https://eu.globalstar.com/en/



Figur 2: Når strømmen går, virker ikke brukerutstyret

5.2 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 virksomhet kan sikre seg mot.



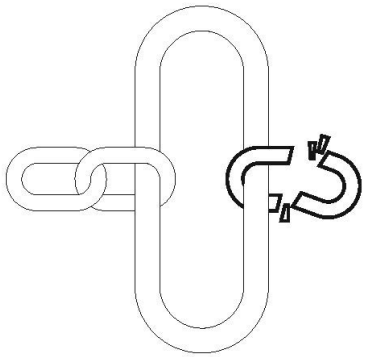
Figur 3: Tilgangsnettet kan rammes av linjebrudd

5.3 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 kan få konsekvenser for mange brukere og store områder. De siste årene har det forekommet logiske feil som har forårsaket utfall landsomfattende utfall.



Figur 4: Logiske feil kan slå ut en hel tjeneste i kjernenettet

Villede handlinger som for eksempel cyberangrep er en risiko som hører hjemme i en ROS. Cyberkriminalitet dreier seg vanligvis om å overvåke og skaffe seg uautorisert tilgang til tjenester og systemer. Cyberangrep kan ramme både tjenester og ekominfrastruktur. Det finnes mange måter å gjennomføre et cyberangrep på. Målet til angriperen kan være alt fra digital spionasje til pengeutpressing og sabotasje.

Tilgangsnett og transportnett er i økende grad basert på IP-teknologi og standardisert utstyr. Trenden er at IP tar over for gamle transmisjonsmekanismer. Dette gir en økt sårbarhet for cyberangrep. Risikoen for angrep på ekominfrastruktur, og dermed forårsake ekomutfall, anses som økende.

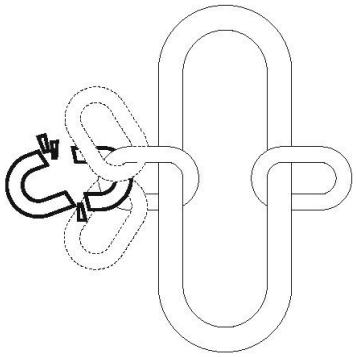
5.4 Unormalt stor trafikk

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.

Unormalt stor trafikk kan i noen tilfeller skyldes villede handlinger som tjenestenektangrep (DDoS[10]). Ved slike angrep sendes forstyrrende trafikk mot visse IP-adresser, gjerne et sammenhengende spenn av adresser. Virksomheter som har tjenester som nås via Internett er utsatt for slike angrep, men også nettelementer hos en ekomtilbyder kan rammes. Effekten av tjenestenektangrep er at tjenestemaskiner «bombarderes» av trafikk fra nettet og dermed ikke blir i stand til å betjene reell trafikk.



Figur 5: Ved store hendelser kan kapasiteten bli sprengt ved at for mange kjemper om en begrenset ressurs

5.5 Sårbarheter i ekomnett og -tjenester

For å møte samfunnets avhengighet, bygges mye sikkerhet inn i selve ekominfrastrukturen. Alternative framføringsveier mellom punkter i nettet, dublering av utstyr og reservestrøm til det

[10] Distributed Denial of Service

viktigste utstyret, er typiske tiltak operatørene gjør for å sikre nettene sine. Slik sett blir infrastrukturen samlet sett mer robust.

En ekomtjeneste er gjerne avhengig av andre tjenester som leveres av ulike underleverandører. Slike avhengigheter skaper *komplekse verdikjeder*[11]. Hvis en tjeneste i en slik verdikjede svikter vil alle tjenestene som har en avhengighet til denne tjenesten bli rammet.

Noen egenskaper ved dagens nett representerer sårbarheter som er verd å merke seg. Med sårbarheter menes her egenskaper som gjør nettene sårbare for truslene beskrevet i 5.1– 5.4. Disse kan oppsummeres til:

- Bredbånd og mobiltelefoni er avhengig av strøm lokalt for å virke, mens tradisjonell fasttelefoni fikk strøm fra nærmeste sentral.
- 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 i ekominfrastrukturen. Ekomtjenester er avhengige av at sentrale elementer i nettet fungerer og kan kommunisere med den enkelte bruker. For eksempel kan programvarefeil eller konfigurasjonsfeil i kritiske funksjoner i en tilbyders kjernenett ramme hele tjenesten.
  I dagens marked er ekomtjenester gjerne integrert i pakkeløsninger. Private husholdninger kan for eksempel kjøpe en pakkeløsning for bredbånd, TV, e-post og skylagring av samme leverandør. En trend i hele samfunnet er en økende bruk av skytjenester både for datalagring og tjenesteproduksjon. Etter hvert som ekomtjenestene utvikles og blir stadig mer avanserte, øker også kompleksiteten til de underliggende infrastrukturene og systemene. For at en enkelt ekomtjeneste skal fungere, er man avhengig av at alle ledd i disse verdikjedene fungerer. Det er imidlertid utfordrende å holde oversikten over og ha kontroll på alle potensielle sårbarheter.
- Mobilnettene er ikke dimensjonert for ekstreme lokale trafikktopper. 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.

[11] NOU 2015:13. «Digital sårbarhet – sikkert samfunn» Beskriver komplekse verdikjeder og sårbarheter.

6 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 virksomheter redusere risikoen for at ekomtjenestene de er avhengig av, blir utilgjengelige.

Med utgangspunkt i den enkle modellen av ekomnettene (figur 1) og truslene over (figurene 2-5), vil effektive tiltak være

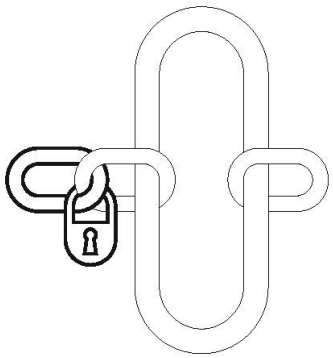
a) lokale reserveløsninger for strøm
b) flere uavhengige forbindelser i tilgangsnettene
c) abonnement hos flere tilbydere med uavhengige kjernenett
d) prioritetsabonnement i mobilnett

6.1 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. Det har store konsekvenser for virksomheter 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[12] 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 mot korte brudd og gir vern mot overspenning som kan forekomme for eksempel ved lynnedslag.

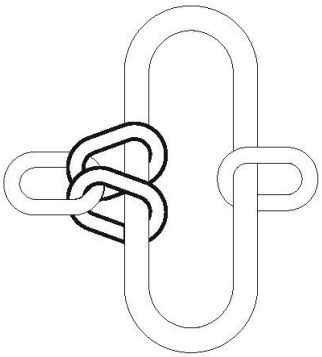
[12] Vanlig brukt engelsk betegnelse: Uninterruptible Power Supply - UPS



Figur 6: Ekstra strømforsyning reduserer sårbarheten lokalt

6.2 Flere uavhengige forbindelser

Det finnes nesten 150 tilbydere[13] av fast bredbånd i Norge. Mange av disse er lokale, for eksempel kraftselskaper, og har infrastruktur bare i et begrenset område. For den enkelte virksomhet vil det typisk være et par alternativer. 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.



Figur 7: Flere tilgangsnett reduserer sårbarheten for linjebrudd

[13] Oversikt over tilbydere registrert hos Nkom pr februar 2016

6.2.1 Telefoni

For taletjeneste vil et tiltak være å ha både fasttelefon og mobiltelefon. Fasttelefon kan være analog, men de fleste virksomheter benytter i dag IP-baserte løsninger. Den tradisjonelle fasttelefonien benytter kobbernettet mens IP-basert fasttelefoni benytter samme tilgangsnett som for bredbånd. Hvis man ønsker ekstra redundans for fasttelefoni kan to ulike tilgangsnett være en løsning.

6.2.2 Mobil datakommunikasjon

Alle mobilnettene som formidler tale, tilbyr også mobilt bredbånd i sine nett. 4G teknologien tilbyr hastigheter opp mot det man får på fast bredbånd. Avhengig av lokal kapasitet kan mobilt bredbånd fungere som backup hvis fast bredbånd faller ut.

En teknisk forskjell mellom det nettet ICE har for mobilt bredbånd og de andre mobilnettene, er at noen basestasjoner i ICE-nettet sender med lavere frekvenser. Dette medfører at signalet mellom disse basestasjonene og telefon/modem når frem over lengre avstander. En slik 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.

6.2.3 Bredbånd

Fast bredbånd leveres de fleste steder over både fiber- og kobberkabler. Statistikk for 2015[14] viser at 94 % av husstandene i landet kan velge mellom tre eller flere tilgangsteknologier for bredbånd og 99 % minst to. Selv om en virksomhet har sin hovedforbindelse for bredbånd på fiber, kan det være en rimelig forholdsregel å beholde eller eventuelt tegne 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.

6.2.4 Faste samband

En større virksomhet eller 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 virksomheten 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

[14] Bredbåndsdekning 2015 utarbeidet av Nexia for Nasjonal kommunikasjonsmyndighet september 2015

ruting, være aktuelt. Spredt ruting vil si at to samband mellom tilknytningspunkter i transportnettet, legges på uavhengige 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 ikke forbindelser som er uavhengige på bestillingspunktet, over tid kan havne i samme føringsvei eller bli avhengig av felles ressurser.

6.3 Flere uavhengige abonnement

6.3.1 Telefoni

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.

6.3.2 Mobilabonnement

Det er flere fysiske mobilnett i Norge. Et enkelt og rimelig tiltak er derfor 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 Telia 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 Phonero.

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.

6.3.3 Bredbåndsabonnement

Ovenfor 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 større virksomhet med flere lokasjoner kan en løsning være å benytte separate internettilknytninger basert på funksjon og sårbarhet til lokasjonene. Et eksempel er kommuner der sentraladministrasjonen, institusjoner, skoler og biblioteker er 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 Internettilknytninger 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.

6.3.4 Andre tjenester

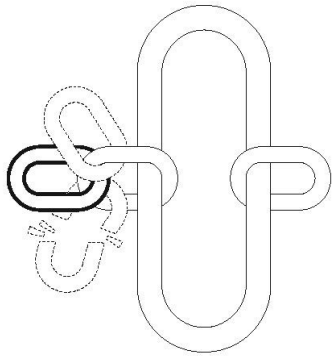
I mange tilfeller settes drift av applikasjoner ut til eksterne leverandører. Når de eksterne leverandørene tilbyr slik drift i storskala datasentre på Internett, omtales det gjerne som skytjenester. E-post regnes vanligvis ikke som en ekomtjeneste, men det er uansett en viktig tjeneste for en virksomhet. Derfor bør en sikre tilgjengelighet for den på tilsvarende måte som for ekomtjenester. For tilgjengelighet alene, kunne skybasert e-postleveranse hatt attraktive egenskaper. 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 tjenestemaskiner for e-post plassert på geografisk adskilte steder og gjerne i ulike operatørers IP-nett. Tjenestemaskiner som speiler hverandre reduserer sårbarheten for enkeltfeil og gir større motstandsdyktighet mot tjenestenektangrep.

Figur 8: Ved å abonnere på uavhengige tjenester, vil en ikke så lett bli slått ut av feil i kjernenettet

6.4 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 være et tilbud til virksomheter som har ansvar for kritiske funksjoner i samfunnet. Begrensningen på antall brukere i ordningen innebærer at den enkelte 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 Nkom om godkjenning via Altinn før de kan tegne abonnement. Tilbydere vil normalt kreve at prioritet knyttes til bedriftsabonnement. Se Nkoms hjemmeside nkom.no for mer informasjon om hvordan skaffe prioritetsabonnement. Relevant informasjon kommer opp ved å søke på nøkkelordet «prioritet».



Figur 9: Med prioritetsabonnement oppnår en å komme gjennom selv når nettet er fullt – om nødvendig på bekostning av uprioritert trafikk

6.5 Satellittkommunikasjon

Så lenge brukeren har sikret strømtilførsel til sin egen satellittelefon vil kommunikasjon via satellitt ikke påvirkes av linjebrudd eller utfall av elektrisk kraft i eget nærområde. 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 7.5) enn for det generelle behovet for robuste ekomløsninger.

6.6 Maskin-til-maskin-løsninger

Det finnes produkter og systemer som benytter seg av maskin-til-maskin-kommunikasjon (M2M) via mobilnettet. Mest utbredt er systemer for alarmer og styring av strøm. Kommuner har for eksempel brukere av trygghetsalarmer. Leverandør av selve M2M-løsningene og leverandør av mobiltjenesten som løsningen baserer ser på er gjerne ikke de samme. Drift av slike løsninger kan derfor være ekstra utfordrende. M2M-løsninger benytter 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 og hvilke begrensninger disse har. Benyttes GSM-basert mobildata er datahastigheten svært begrenset sammenlignet med 3G og 4G mobildata. På sikt vil eldre teknologier fases ut blant annet for å frigi frekvenser til nye systemer. Mest sannsynlig vil 3G fases ut før 2G ettersom mange M2M systemer fortsatt benytter GSM.

6.7 Avtal tjenestekvalitet og -sikkerhet med tilbyder

Det er viktig å diskutere kvalitet og sikkerhet med den eller de tilbyderne som er valgt for leveranse av elektroniske kommunikasjonstjenester. En tilbyder må kunne redegjøre for sikkerheten i alle kritiske ledd som tjenesten består av. Virksomheten må selv også avklare hvilke tilbydere har ansvar for hvilke deler av en leveranses verdikjede. For eksempel kan det være forskjellige parter som har ansvar for tilgangen til en tjeneste (f. eks. en ISP) og produksjon av selve tjenesten (f.eks. en telefoniløsning). Slike avtaler betegnes ofte som SLA (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.

En god SLA-mal kan gjøre nytte som sjekkliste der hvor partene velger en annen måte å dokumentere kontraktsforholdet på.

6.8 Beredskap mot cyberhendelser

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

Alvorlige datainnbrudd er komplekse og noe de færreste virksomheter har erfaring og kapasitet til å håndtere selv. Avhengig av virksomhetens verdier og kritikalitet anbefales det å knytte seg opp mot eksterne fagmiljøer som har nødvendig kompetanse og kapasitet til håndtering av alvorlige sikkerhetshendelser. Dette kan være både private sikkerhetsselskaper og private/offentlige sektorvise responsmiljøer som KraftCERT, FinansCERT osv.

7 Ekom i krisesituasjoner

I planlegging av kriseberedskap må virksomhetene 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 gir ut veiledninger om risiko- og krisekommunikasjon som særlig legger vekt på kommunikasjon ut mot befolkningen. Dette kapitlet omhandler praktiske råd til bruk av ekom i håndtering av en krise når tilgangen til de vanlige ekomtjenestene er borte eller sterkt redusert.

7.1 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.

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.2 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.

7.3 Informasjonsdeling

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.

Aktører som for eksempel Google og Apple tilbyr gratis skytjenester for e-post og deling av dokumenter og bilder. I en krisesituasjon kan slike løsninger benyttes som et alternativ når tilgjengelighet er det overordnede kravet, selv om slike tjenester ikke skulle oppfylle virksomhetens normale krav til sikkerhet. I alle tilfeller må adresseinformasjonen være dokumentert og tilgjengelig for å kunne benyttes. Under den store skogbrannen i Västmanland i Sverige i 2014 ble Googles skytjeneste benyttet av den lokale kriseledelsen for å komme raskt i gang med informasjonsdeling under slukningsarbeidet.

7.4 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.

7.5 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 tilfeller kan det være hensiktsmessig å basere seg på begge typer system.

Noen telefoner for systemet Globalstar kan ta SIM-kort slik at den samme telefonen også kan brukes mot et GSM-nett. I de regionene hvor Globalstar har samtrafikkavtale med lokale mobilnettoperatører vil det være mulig å bruke samme telefonnummer både ved bruk av GSM-nett og satellittnett. Tilbyderen 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. Nkom 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 (jf. Inmarsat og Thuraya).

For faste punkt med tilgang på strøm vil det beste alternativet være en toveis satellittforbindelse gjennom en fastmontert parabolantenne. En slik løsning har kapasitet på mange megabits per sekund.

7.6 Kommunikasjon og koordinering med andre kriseaktører

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. Enkelte satellittelefoner (se over) kan brukes til å få tilgang til Internett i tillegg til ordinært talesamband. Som en del av beredskapen bør det finnes rutiner for bruk av krisestøtteverktøy over alternative samband. Det er viktig at det er etablert rutiner for slik kommunikasjon på forhånd.

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.

7.7 Nødnett

Nødnett, som ble tatt i bruk i hele landet 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), men også private og offentlige virksomheter som drifter eller har ansvar for kritisk infrastruktur eller utøver viktige samfunnsfunksjoner kan søke DNK om å bli bruker. 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 virksomheter 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. Virksomheter vil måtte betale for egne radiohåndsett i tillegg til en abonnementsavgift. Tilgang til Nødnett kan være nyttig for å samhandle med andre aktører som for eksempel kommuner og fylkesmenn.

7.8 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 hjemmesider og sosiale medier være viktige kanaler for dette. De vanlige kanalene kan imidlertid være utilgjengelige og en beredskapsplan bør derfor 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 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.