Nkom ROS

Nasjonal kommunikasjonsmyndigheit si risiko- og sårbarheitsanalyse

2025

Nasjonal kommunikasjonsmyndigheit


N
K

Innhold

SAMANDRAG

I denne risiko- og sårbarheitsanalysen (ROS-analysen) vurderer Nasjonal kommunikasjonsmyndigheit (Nkom) risiko- og trusselbiletet i ekomsektoren, med særleg søkjelys på det digitale trusselbiletet og at det blir meir sikkerheitspolitisk usikkert. Kritisk infrastruktur i Noreg står framleis overfor vedvarande høg risiko, og samfunnet si evne til å fungere er i stor grad avhengig av både fysisk og digital infrastruktur. Svikt i denne infrastrukturen og systema vil medføre alvorlege konsekvensar for leveransen av kritiske varer og tenester som innbyggjarane og styresmakter er avhengige av.

Dei største utfalla vi har sett dei siste åra skuldast ekstremvêr og feil ved gjennomføring av planlagd arbeid hos ekomtilbydarane. Ekomnetta er robuste og tåler mykje uvêr. Samtidig viser ekstremvêra Hans, Ingunn, Amy og stormen i Trøndelag januar 2025 at fiberinfrastrukturen og spesielt kraftforsyninga er tydeleg sårbar. Hovudårsaka til dei omfattande utfalla av ekom for begge hendingane i 2025 var tap av ekstern straumforsyning frå lokale kraftselskap. For å stå imot denne typen utfall må straumnettet bli meir robust, ekomnetta må få meir reservestraum, og midlertidig dekning må kunne etablerast raskare.

Store og langvarige straumbrot er utfordrande å handtere for ekomsektoren og samfunnet elles. Det er ei grense for kor mykje samfunnet kan dimensjonere talet på mobile reservestraumsaggregat i beredskap og den generelle reservestraumsforsyninga til samfunnskritiske funskjoner utan at det medfører urimeleg store kostnader for den enkelte verksemd og sektorar. Kraftsektoren må derfor sikre redundansen i kraftforsyninga betre for å handtere ekstremvêr og kriser.

Samtidig må ekomsektoren også styrke reservestraumskapasiteten i ekomnetta for å kunne stå imot kortare kraftutfall og fiberbrot ved ekstremvêr. Nkom meiner at ekomsektoren må styrke evna si til å handtere lokale og kortvarige utfall av ekstern kraftforsyning betre, fram til 8-24 timar, medan kraftnettselskapa må sikre at talet på og omfanget på kraftutfall utover dette blir avgrensa vesentleg meir enn i dag. Fleire basestasjonar må få lengre reservestraumsforsyning og dei må sikrast fleire føringsvegar for transmisjon. Det forsterka ekomprogrammet må forserast, fleire basestasjonar med 12 til 24 timer reservestraum er nødvendig og det bør vurderast om det generelle kravet til reservestraumsforsyning til basestasjonar må aukast ytterlegare. Samtidig må fleire forsterkningstiltak av fiberinfrastrukturen gjennomførast for å auke redundansen og evna til å motstå store hendingar.

Erfaringar frå Ukraina viser korleis kraftsektoren blir angripen for å påverke samfunnet og andre kritiske samfunnsfunksjonar. Vidare viser erfaringane at det å ha definert strukturar for samvirke og rutinar for gjenoppretting av kraft og ekom på førehand er viktigare enn prioritering av enkeltlokasjonar. Dette fordi situasjonen er såpass flyktig og under konstant endring, at å ha ei effektiv verktøykasse er meir føremålstenleg enn detaljerte planar. Dette kan overførast til norske forhold. Det er viktig at det blir skapt arenaer for samhandling som fylkesberedskapsråd, ekomberedskapsråd og direkte samhandling mellom ekomtilbydarar og kraftselskap som er øvd og testa.

Planlagt arbeid i fast- og mobilnett skjer i stadig meir komplekse miljø, med mange leverandørar og system som er tett kopla saman. Dette gjer det vanskeleg å ha full oversikt over kva som er avhengig av kva, og konsekvensar. Feil kan raskt spreie seg, og endringar kan gi uventa ringverknader som krev tilbakerulling. Nkom ser at mangelfulle risikovurderingar og

organisatorisk svikt ofte ligg bak slike hendingar, forsterka av fragmentert ansvar i leverandørkjeder. Dette gjer gode rutinar for risikovurdering og endringshandtering avgjerande.

Nkoms ekom ROS 2024 peika på cybertrusselen som den mest alvorlege trusselen mot ekom-infrastrukturen, med stort skadepotensial. Dette biletet er framleis gjeldande. I analysen for dette året byggjer vi vidare på denne vurderinga, samtidig som vi legg til grunn den skjerpa sikkerheitspolitiske situasjonen. Dette dannar eit alvorleg bakteppe for ROS-analysen for dette året.

Innsidetrusselen i Noreg har auka. Innsiderisiko er vanskeleg å verne seg mot, og når ein ser på konsekvensane av uhell i ekomsektoren, kan ein gå ut frå at skadepotensialet ved ei handling utført med vilje kunne blitt endå meir alvorleg. Det er mykje som er mogleg for ein innsidar, sidan vedkomande allereie er innanfor fleire sikkerheitsbarrierar både i det fysiske og det logiske domenet. Dette kan auke sjansen for å lukkast med å gjennomføre hendingar som sabotasje, informasjons¬innhenting, planting av skadevare og destruktive angrep. Det har i lengre tid vore utfordrande å innhente tilstrekkeleg informasjon for kritisk utenlandsk personell – inkludert frå andre nordiske land. Etter at Sverige og Finland har tredd inn i Nato bør det være mogleg å få til effektive ordningar med sikkerheitsklarering på tvers av nordiske land.

Denne ROS-analysen har vidare søkjelys på kritiske utfordringar slik som kvar ein er sårbar i verdikjeda og frekvensforstyrringar mot radiobaserte signal for posisjon, navigasjon og tid (PNT-signal). Riktig opplysning av posisjon og tid er avgjerande for funksjonen til ekomtenester, samt for infrastruktur og system i andre sektorar. Ein kan bli utnytta der ein er sårbar for å manipulere tids- og posisjons-opplysningar. Samtidig blir cyberangrep stadig meir sofistikerte og profesjonelle, mellom anna på grunn av kunstig intelligens (KI). Dette har auka suksessraten for økonomisk motiverte cyberangrep kraftig.

Den skjerpa sikkerheitspolitiske situasjonen gjer at vi må stille strengare krav til å vere robust og motstandsdyktig i våre digitale infrastrukturar. Både den ferske rapporten frå Riksrevisjonen og den nye nasjonale sikkerheitsplanen peikar tydeleg på at vi ikkje er på det nivået vi må vere når det gjeld sikkerheit og beredskap. Det er eit stort gap mellom dagens status og det kravde sikkerheitsnivået – eit gap som må lukkast gjennom høgare tempo og meir målretta innsats. Nkom kjenner seg igjen i funna og vurderingane i dei to rapportane, og ser dei same utfordringane for elektronisk kommunikasjon. Regjeringa sin nye nasjonale sikkerheitsplan vil vere eit godt steg på vegen for å tette dette gapet.

For å sikre forsvarleg sikkerheit og beredskap må risiko- og sårbarheitsanalysene til verksemdene oppdaterast i tråd med utviklinga av den sikkerheitspolitiske situasjonen og trusselvurderingane frå dei hemmelege tenestene. Ein må ta omsyn til både tilsikta og utilsikta hendingar – logiske like fullt som fysiske. Det må vere krav til eit tett og forpliktande samarbeid mellom styresmakter, bransjeaktørar, og både offentlege og private verksemder, for å nå dei nasjonale måla. Ingen aktør kan løfte dette åleine – alle må bidra, både med ressursar, kompetanse og investeringar. Ein felles innsats er nødvendig for å byggje eit digitalt Noreg som er trygt, robust og motstandsdyktig – også i møte med framtidige kriser.

Foto: Anders Martinsen

1 INNLEIING OG BAKTEPPE FOR NKOM ROS 2025

Nasjonal kommunikasjonsmyndigheit (Nkom) har ansvar for å forvalte elektronisk kommunikasjon (ekom) i Noreg. I tråd med hovudinstruksen for Nkom er det gjennomført ei risiko- og sårbarheitsanalyse for 2025. Denne rapporten er eit avgrensa utdrag frå den fullstendige risiko- og sårbarheitsanalysen. Den komplette versjonen er gradert og tilgjengeleg berre på avgrensa nett. Dette dokumentet er den aggregerte, offentleg tilgjengelege utgåva og er utarbeidd for å kunne delast utan at sikkerheiten blir kompromittert.

Rapporten tek utgangspunkt i den sikkerheits-politiske situasjonen og korleis denne påverkar ulike område innan ekomsektoren. I tillegg vurderer analysen risiko knytt til klimaendringar, ekstremvêr og planlagt arbeid i nettet.

Målgruppa for analysen er Digitaliserings- og forvaltningsdepartementet, andre departement og styresmakter, statsforvaltarar, ekomtilbydarar og operatørar av datasenter.

Dei opne trusselvurderingane frå EOS-tenestene (februar 2025) peikar på ei verd som blir stadig meir uforutsigbar og farleg. Trusselen mot sikkerheita til Noreg er aukande, mellom anna som følgje av den aggressive utanrikspolitikken frå Russland og den vedvarande konflikten med Vesten.

Krigen i Ukraina held fram, utan teikn til ei varig løysing til fred. Kreml ser det som nyttig å destabilisere vestlege økonomiar, industri og forsvarsevne gjennom hybride verkemiddel som cyberangrep og sabotasje. I 2024 kom over 40 sabotasjeforsøk i Europa for dagen, og russiske aktørar sine handlingar blir stadig meir uføreseielege. Våren 2025 klarte russiskstøtta hackarar å manipulere ein port i eit damanlegg i Noreg. Dette medførte auka vassføring i ei elv på Vestlandet, men utan alvorlege konsekvensar.

Sjølv om eit fullskala militært angrep mot Noreg blir vurdert som lite sannsynleg, må samfunnet førebu seg på ein aukande risiko for både digitale og fysiske truslar mot kritisk infrastruktur. Døme på sabotasjeforsøk inkluderer digitale angrep mot europeiske jernbaner, fysiske innbrot i vasskraftverk i Tyskland, Sverige og Finland, angrep mot global flyfrakt og omfattande brannstiftingar, til dømes i Warszawa i Polen.

I samband med invasjonen av Ukraina har Russland vist både vilje og evne til å forstyrre kritisk infrastruktur. Dei siste åra har det blitt rapportert om omfattande GNSS-forstyrringar i Finnmark. Ved å påverke både tid og posisjon kan slike angrep få alvorlege konsekvensar for navigasjon og logistikk.

Aust-Finnmark har i lengre tid opplevd daglege GPS-forstyrringar, og liknande hendingar er rapportert på Svalbard og i Barentshavet utan kjent årsak. Jamming kan påverke navigasjons-tenester som GPS i køyretøy, mobilkart og treningsutstyr. Sjølv om ingen andre delar av landet er særskilt utsett, bør ein vurdere beredskap for svikt i digitale navigasjons-system. Den digitale infrastrukturen er avhengig av satellittbaserte system, som er sårbare trass i effektiviteten. Dette understrekar kor viktig det er med reserveløysingar for kritiske innsatsfaktorar i eigen tenesteproduksjon og nasjonal beredskap.

Det er avgjerande at vi tek dette på alvor og set søkjelys på å stramme inn føringane for kva som er meint med forsvarleg sikring. Samtidig må krava til å vere robust, krav til beredskap og tilhøyrande beredskapsressursar i ekomsektoren skjerpast.

Samfunnet blir stadig meir digitalisert, og Noreg blir i dag rekna som eitt av dei mest digitaliserte landa i verda. Digitaliseringa krev ein robust og trygg digital infrastruktur som fundament for både daglegliv og kritiske samfunnsfunksjonar. Samtidig aukar den digitale trusselen mot Noreg. Hackergrupper, kriminelle aktørar og aktivistar gjennomfører stadig fleire cyberangrep mot verksemder og styresmakter. Den aukande offensive haldninga frå Russland overfor NATO gjer at destruktive cyberangrep blir meir sannsynlege i samband med politiske konfliktar som omhandlar sikring.

Totalberedskapsmeldinga 2025 gjer det tydeleg at det er behov for eit samordna og systematisk beredskapsarbeid. Tiltak som styrkjer motstandskrafta til samfunnet mot digitale og samansette truslar, utgjer ein sentral del av bodskapen. Meldinga peikar også på at nivået av sikring i fredstid også må tole påkjenningar i ein krigssituasjon. Det er viktig å ta på alvor at ekom er ein kritisk del av totalforsvaret. Fleire punkt i meldinga omhandlar direkte vern av kritisk infrastruktur, der ekom utgjer ein viktig del. Samtidig spelar ekom ei avgjerande rolle i andre beredskapstiltak, sjølv der det ikkje eksplisitt blir nemnt som hovudfaktor. Ekom er også sterkt avhengig av andre beredskapstiltak, og då særleg tilgang på straum.

Eit tydeleg døme på ekom si viktige rolle er ved evakuering. Totalberedskapsmeldinga understrekar at det må vere tilstrekkeleg ekom for å kunne handtere slike situasjonar effektivt. Ein føresetnad for evakuering er kontinuerleg og påliteleg kommunikasjon mellom beredskapsaktørar, styresmakter og innbyggjarar. Det er usikkert når tid og kvar slike evakueringar vil finne stad, men vi må likevel planleggje for at dei kan bli nødvendige. Dette krev robuste og motstandsdyktige kommunikasjonsløysingar som fungerer sjølv under krevjande forhold, inkludert ved sabotasje, cyberangrep eller bortfall av infrastruktur.

Riksrevisjonen sin rapport "Totalforsvaret i tryggleikspolitisk krise og krig" avdekkjer alvorlege svakheiter i Noregs evne til å handtere ei sikkerheitspolitisk krise eller krig. Rapporten peikar på at det framleis manglar grunnleggjande føresetnader for eit velfungerande totalforsvar, trass i satsinga sidan 2016. Særleg alvorlege er funna knytt til elektronisk kommunikasjon og kritisk infrastruktur, der det manglar oversikt over planverk for sivil støtte til Forsvaret. Kommunar og andre sivile aktørar planlegg i liten grad for krig. Dei får ikkje nødvendig informasjon, kjenner ikkje Forsvaret sine behov og øver ikkje på relevante scenario. Dette gjer at vi i dag ikkje er tilstrekkeleg budde på å møte ein alvorleg sikkerheitspolitisk situasjon.

Nasjonal sikkerheitsplan for digital infrastruktur legg vekt på å styrkje sikkerheit og beredskap for kritisk digital infrastruktur i fred, krise og krig. Planen peikar på behovet for meir robuste mobil- og breibandsnett, betre nasjonal kontroll, og tettare samarbeid mellom styresmakter og bransje for å sikre at Noreg kan oppretthalde viktige samfunnsfunksjonar under alle forhold. Digitaliseringa gjer det mykje mogleg med effektivisering og innovasjon, men det gjer også at ein blir sårbar på nye måtar. Stadig fleire kritiske samfunnstenester blir overført til kommersielle mobil- og breibandsnett, og den framtidige naud- og beredskaps-kommunikasjonen (Nødnett) skal byggjast på desse. Dette aukar krava til sikkerheit, det å vere robust og samhandling mellom aktørane som forvaltar, driv og brukar infrastrukturen.

Med dagens sikkerheitspolitiske situasjon som bakgrunn, skildrar denne rapporten verdiar og område innan elektronisk kommunikasjon som må vernast, saman med Nkom sine vurderingar og tilrådde risikoreduserande tiltak. Dei overordna samfunnsverdiane som skal vernast – økonomi,

liv og helse, samfunnsstabilitet, demokratiske verdiar og styringsevne, samt natur og kultur – er ikkje nærare behandla i denne versjonen, men blir gjennomgått i den graderte utgåva. Fleire av desse verdiane er tett knytte til elektronisk kommunikasjon.

Det er viktig at norske aktørar vågar å ta inn over seg at ein må bu seg på hendingar i det breie krisespekteret, inkludert scenario som omhandlar verstefallshendingar. Noreg må vere budd på ei eskalering i bruken av hybride verkemiddel mot norske tryggingsinteresser. Dette ber i seg at ein har kartlagt verdiar, truslar og kvar ein er sårbar grundig, og prioriterer tilstrekkelege ressursar for å kunne arbeide med tiltak og verktøy som kan avgrense og handtere hendingar høgt i krisespekteret.

Både på regionalt og nasjonalt nivå er det viktig å prioritere risiko- og sårbarheitsanalysar, då dei legg grunnlaget for målretta tiltak og styrkt beredskap. Gjennom planlegging, auka søkjelys på krav til forsvarleg sikring og målretta innsats kan vi saman byggje ein tryggare og meir motstandsdyktig digital grunnmur for framtida. Nkom ROS 2025 tek for seg risikoar og sårbarheiter knytt til elektronisk kommunikasjon. Dokumentet har som mål å identifisere potensielle truslar og svake punkt ved å bruke tidlegare erfaringar og eksisterande kunnskap. Historiske hendingar kan ikkje åleine tene som ein påliteleg indikator for framtidige truslar i eit stadig meir komplisert trusselbilete. Teknologisk utvikling, det at vi blir meir digitalt sårbare og kombinerte truslar krev ein ny måte å vurdere og handtere risiko på. Informasjonskrigføring, påverknadsoperasjonar og avanserte digitale angrep er blitt ein del av dagens utfordringar mot sikring.

1.1 SENTRALE AKTØRAR I EKOMSEKTOREN

I ekomsektoren har fleire sentrale aktørar ei avgjerande rolle i å sikre robust og påliteleg elektronisk kommunikasjon.

Digitaliserings- og forvaltningsdepartementet (DFD)
DFD har hovudansvaret for politikken og forvaltinga av ekomsektoren i Noreg. Departementet gir føringar og krav til Nkom gjennom ekomlova, forskrifter, instruksar og tildelingsbrev. DFD har ei overordna rolle i å sikre at sektoren følgjer nasjonale krav til sikring og å vere robust[1]. Departementa representerer det strategiske nivået innan sikkerheit og beredskap i ekomsektoren.

Nasjonal kommunikasjonsmyndigheit (Nkom)
Nkom er utøvande styresmakt underlagt DFD og har ansvar for sikkerheit og beredskap i ekomnetta. Styresmakta overvakar og handterer hendingar heile døgnet gjennom ei dedikert beredskapsvakt og spektrumsavdelinga har eit spesielt ansvar for å handtere hendingar som relaterer seg til satellittbaserte tenester og frekvensforstyrrelser. Nkom driv òg EkomCERT som er sektoren sitt responsteam med både nasjonale og internasjonale kontaktpunkt. I tillegg koordinerer Nkom beredskapsarbeidet med andre sektorar og aktørar[2].

Ekomtilbydarar
Ekomtilbydarar, definert som aktørar som leverer tilgang til elektroniske kommunikasjonsnett og -tenester, har ansvar for forsvarleg drift og beredskap i eigne tenester i samsvar med ekomlova § 1-5. Dette ber i seg at tilbydarane må prioritere viktige samfunnsfunksjonar og sørgje for at naudkommunikasjon blir halden oppe under alle forhold[3].

[1] Digitaliserings- og forvaltningsdepartementet - regjeringen.no
[2] Kva gjer Nkom – Nkom
[3] Lov om elektronisk kommunikasjon

Foto: Gunstein Myhre

1.2 OMGREP BRUKT I RAPPORTEN

I denne rapporten blir det nytta fleire omgrep innan elektroniske kommunikasjonssystem og andre teknologiske område. Forklaring på nokre av dei viktigaste er:

Forsvarleg sikring handlar om evna til å stå imot hendingar som medfører eller kan medføre brot på tilgjenge, autentisitet, integritet eller konfidensialitet i elektroniske kommunikasjons¬nett eller -tenester. Dette gjeld data som både er lagra, overførte og handtert, samt tenester som blir tilbode gjennom eller gjort tilgjengelege via slike nett eller tenester[4]. Forsvarleg sikring er ein rettsleg standard som skal utviklast over tid i takt med teknologisk utvikling, marknadstilhøve og samfunnsbehov.

Samfunnssikkerheit handlar om evna til å verne samfunnet mot og handtere hendingar som truar viktige verdiar og funksjonar, eller set liv og helse i fare. Slike hendingar kan skuldast naturkatastrofar, tekniske eller menneskelege feil, eller vere resultat av medvitne handlingar[5]. I hovudinstruksen for Nkom går det fram at Nkom har ei rolle og eit ansvar i samfunnssikkerheitsarbeidet.

Grunnleggjande nasjonale funksjonar (GNF) er tenester, produksjon og anna verksemd som er så viktige at eit heilt eller delvis bortfall vil påverke staten si evne til å verne nasjonale sikkerheitsinteresser[6].

Risiko handlar alltid om framtidige hendingar og den usikkerheita som følgjer med dei. Usikkerheita gjeld både om ei bestemt, uønska hending vil oppstå og kva konsekvensar ho kan få. Ein forstår dermed risiko som moglege uønska hendingar og dei konsekvensane som følgjer etter.

Eit system eller ekomnett er sett saman av ulike nettverkslag[7] og nettelement. Den fysiske infrastrukturen, som fiberkablar, forsterkarar og anna utstyr som ber dei elektromagnetiske signala ligg nedst. På nettverks- og transportlaga blir IP-nett og ruting sett opp. Øvst, på applikasjonslaget, blir kommunikasjonstenester realisert ut til brukarane. Avhengig av systemet kan dette òg inkludere organisatoriske faktorar, som til dømes personell, rutinar og prosedyrar.

Kritisk infrastruktur er anlegg og system som er nødvendige for å føre vidare eller gjenopprette dei kritiske funksjonane til samfunnet[6].

Sårbarheit er eit uttrykk for dei problema eit system vil få med å fungere når det blir utsett for ei uønska hending, og dei problema systemet får med å gjenopprette sin funksjon etter hendinga. Sårbarheita til systemet kan påverke både sannsynet for og konsekvensane av ei hending[6].

Usikkerheit. Nkom har ingen fast definisjon av usikkerheit, men ser det som ein vesentleg del av risiko. Ein kan uttrykkje usikkerheit på ulike måtar, ofte gjennom utrekning av sannsyn, men slike utrekningar åleine gir ikkje eit fullstendig bilete. Risiko handlar om framtida – noko som kan hende, men som vi ikkje kan vere heilt sikre på når, korleis eller med kva slags konsekvensar. Altså er framtida prinsipielt usikker, og usikkerheit er igjen eit vesentleg element i omgrepet risiko.

Usikkerheit kan delast inn i tre hovudkategoriar:

- *Fortid:* Knytt til kvaliteten på observasjonar og informasjon Nkom har, samt korleis denne er tolka og forstått.
- *Notid:* Gjelder Nkoms nåværande oversikt relatert til ekomnett, tenester, kritisk infrastruktur, aktørar og forståing av trusselbilete, samt samanhengen mellom desse.
- *Framtid:* Framtida er grunnleggande usikker, og denne usikkerheita kan ikkje reduserast.

Beredskap er planlagde og førebyggjande tiltak som gjer ein aktør i stand til å handtere uønska hendingar slik at konsekvensane blir minst mogleg, med mål om at normaltilstanden raskt kan gjenopprettast. Beredskap skal sørgje for at ein kan handtere risiko som ikkje kan førebyggjast[6].

Ekomlova skal bidra til å styrkje sikkerheit og forbrukarane sine rettar innan elektronisk kommunikasjon. Lova set krav til forsvarleg sikring i den digitale infrastrukturen og gir Nkom viktige verktøy for å sikre at brukarane har tilgang til gode, sikre og framtidsretta tenester. Ekomlova byggjer på sektorprinsippet, som ber i seg at ulike departement kan fatte vedtak om kva verksemder innafor sitt ansvarsområde som skal omfattast av lova. Den nye ekomlova tok til å gjelde frå 1. januar 2025 og fører vidare reguleringa av mobil- og breibandtenester, internettbaserte applikasjonar og sosiale medium, og omfattar for første gong spesifikk regulering av datasenter, inkludert krav til registrering, sikkerheitsstyring og beredskapsrutinar[8].

Sikkerheitslova skal bidra til å førebyggje, avdekke og motverke verksemd som truar sikkerheita, samt tilsikta handlingar som direkte eller indirekte kan skade nasjonale sikkerheitsinteresser. Nkom har ansvaret for å føre tilsyn med tilbydarane som er underlagt sikkerheitslova innfor ekomsektoren. Sikkerheitslova byggjer på sektorprinsippet, som ber i seg at ulike departement kan fatte vedtak om kva verksemder innfor sitt ansvarsområde som skal omfattast av sikkerheitslova. Det finst ingen offentleg oversikt over kva selskap i Noreg som er underlagd regelverket[9].

---

[4] Lov om elektronisk kommunikasjon (ekomloven) - Kapittel 3. Sikkerhet og kommunikasjonsvern - Lovdata

[5] Meld. St. 10 (2016-2017) Risiko i et trygt samfunn

[6] Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner

[7] Jamfør OSI-modellen, som består av det fysiske laget (fiber mv.), data link-laget (ethernet mv.), nettverkslaget (IP), transport (TCP, UDP), sesjonslaget (synkronisering, til/fra port, API mv.), presentasjonslaget (syntax samt ulike protokollar og format som SSL, SSH, IMAP og JPEG), og applikasjonslaget (HTTP, FTP, DNS mv.)

[8] nkom.no/aktuelt/stortinget-har-behandlet-ny-ekomlov

[9] nkom.no/sikkerhet-og-beredskap/tilbyders-sikkerhets-og-beredskapsplikter

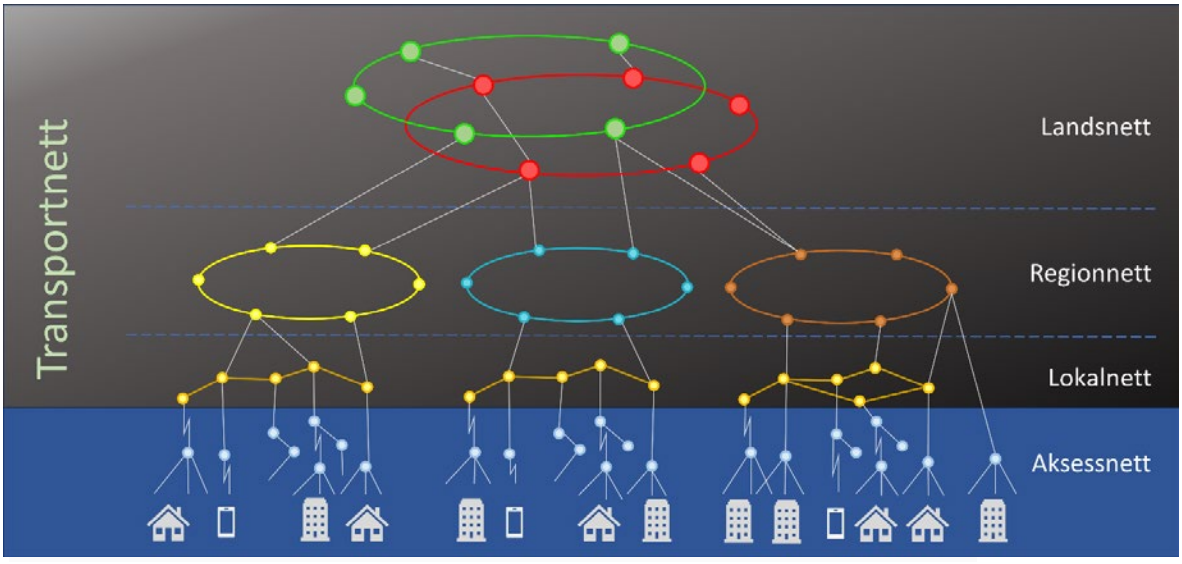
1.3 VERDIAR I EKOMSEKTOREN SOM SKAL VERNAST

Elektroniske kommunikasjonsnett (ekomnett) er system for signaltransport som gjer det mogleg å overføre lyd, tekst, bilete eller andre data ved hjelp av elektromagnetiske signal. Med elektronisk kommunikasjonsteneste meiner ein ei teneste som heilt eller i hovudsak ber i seg formidling av signal i eit elektronisk kommunikasjonsnett, og som vanlegvis blir tilbode mot betaling[10].

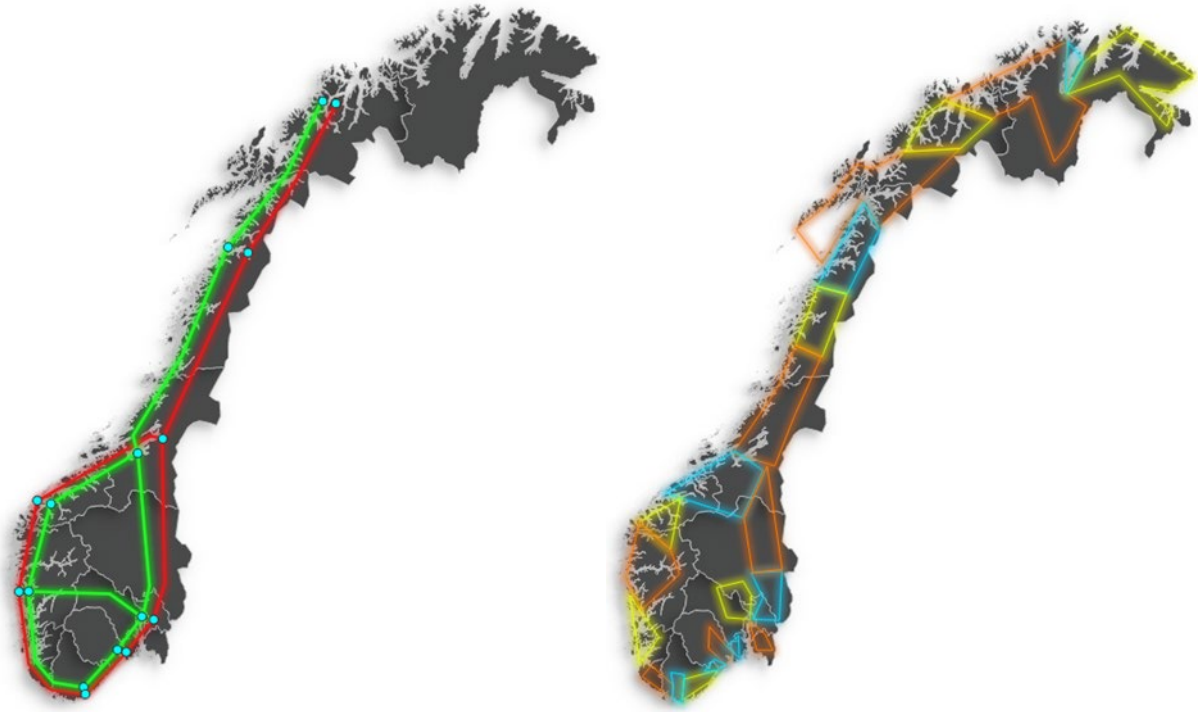
Eit fellestrekk ved dei fleste ekomnetta er at dei er avhengige av underliggjande, landsdekkande transportnett. Fiberkablar med høg kapasitet er nødvendige for å frakte dei elektromagnetiske signala over lange avstandar. Fastnett, mobilnett og andre typar nett er derfor avhengige av den same underliggjande «ryggrads»-infrastrukturen. I nokre tilfelle blir radiolinjer nytta til å overføre elektromagnetiske signal, til dømes der det er vanskeleg eller lite kostnadseffektivt å leggje fiberkablar.

Ekomnett er sett saman av fleire lag i nettverket, som omfattar både fysiske og logiske element. Desse laga verkar saman og gjer det mogleg å levere tenester til sluttbrukar[11].

Nasjonale transportnett blir gjerne delte inn i nivåa lands-, region- og lokalnett (sjå figur 1a og 1b). Dei landsdekkande aktørane har landsnett som bind saman regionnetta og sørgjer for høgkapasitetsforbindingar over dei lengste avstandane. For dei største transportnettaktørane i Noreg går landsnetta nordover til Tromsø, der dei vidare mot nord nyttar region- og lokalnett.



Figur 1a: Skjematisk oppbygging av transportnett og aksessnett



Figur 1b; Døme på landsnett (til venstre) og regionnett (til høgre) for ein landsdekkjande tilbydar

Regionnetta til ein aktør dekkjer som regel eit fylke eller ein større by, og blir òg omtala som metronett. Som vist i figur 2b er regionnetta bygde opp som ringar med høg kapasitet, og er normalt kopla til aktøren sitt landsnett på to ulike punkt. I praksis betyr dette at ein kan nå alle nettverkselement i regionnetta fysisk via minst to separate føringsvegar.

Lokalnetta koplar aksessnetta til regionnetta og dekkjer som regel eit tettstadområde og nærliggjande område. Det finst fleire hundre lokalnett på landsbasis. Desse heng typisk som greiner ut frå tilkoplingspunkt i regionnettet. Utviklinga går i retning av at også lokalnetta får auka redundans.

[10] Lov om elektronisk kommunikasjon (ekomloven) - Lovdata

[11] Tilbyders sikkerhets- og beredskapsplikter - Nkom

2. FARAR, TRUSLAR OG SÅRBARHEITER I EKOMSEKTOREN

Ekom utgjer ein viktig del av samfunnets kritiske infrastruktur og må difor vernast mot eit breitt spekter av farar, truslar og sårbarheiter. Dette kapitelet gjer greie for dei mest sentrale utfordringane knytte til tryggleik og robustheit i ekomsektoren. Dette omfattar både målretta truslar som cyberangrep og svindel, og meir utilsikta hendingar som naturkatastrofar og planlagd arbeid i nettet. Vidare vert sårbarheiter i verdi- og leverandørkjeder belyste, som kan påverke tilgjenge og integritet i kritiske tenester. Det er òg retta merksemd mot satellittbaserte tenester som er grunnleggjande for mange ekomfunksjonar, og som i aukande grad er sårbare for både forstyrringar og manipulering.

Nkom har etablert ei oversikt over årsaker til utfall i ekomsektoren basert på regionale analysar, varslingar til Nkom, oppfølging av hendingar og gjennomførte tilsyn. Internasjonalt samarbeid og samarbeid med andre offentlege etatar dannar òg grunnlag for analysar og vurderingar av risikobiletet.

2.1 RAPPORTERTE HENDINGAR I 2024

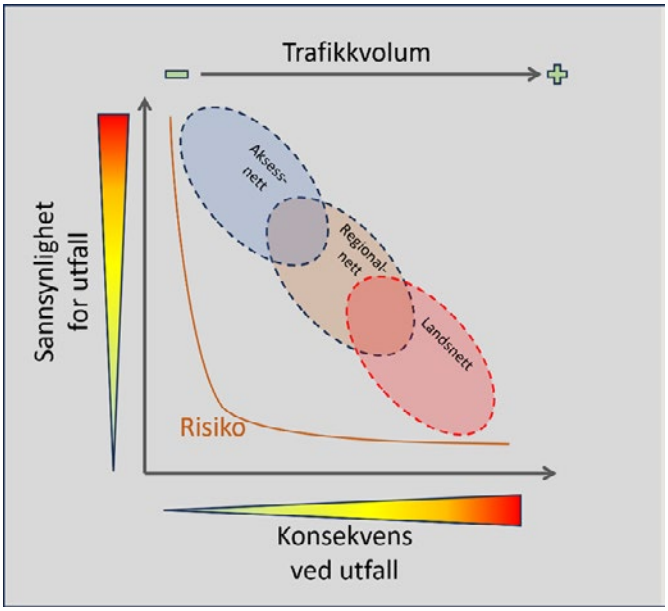
Naturhendingar og straumbrot er blant dei vanlegaste årsakene til avbrot i elektroniske kommunikasjonstenester på fastlandet i Noreg. Stormar, kraftig nedbør, skred og flaum fører ofte til skadar på infrastruktur, og i mange tilfelle er det straumbrotet som utløyser sjølve transmisjonsbrotet. Ekstremvêr som «Amy» hausten 2025 synte kor sårbar ekomsektoren er når straumforsyning fell bort og transmisjonsliner stoppar opp.

Nkom får inn rapportar om større og rapporteringspliktige hendingar. Desse viser at transmisjonsbrot og straumbrot til saman står for om lag to tredelar av feila i tilbydarane sine nett dei siste åra. Mindre, lokale utfall, som til dømes enkeltståande basestasjonar som mistar straum, blir vanlegvis ikkje rapporterte.

Programvarefeil og planlagt arbeid i ekomnetta skil seg ut som ei årsak til meir omfattande og landsdekkande utfall, fordi slike feil ikkje er geografisk avgrensa. Dei mest alvorlege feila Nkom har registrert, har ofte vore knytt til planlagt arbeid i ekomnetta, der endringar har fått uventa ringverknader i større delar av infrastrukturen.

Andre hyppige årsaker er graving, kantslått, brann, utstyrsfeil og menneskelege feil ved drift og endring av netta. Likevel peikar statistikken i éi retning: transmisjonsbrot og straumbrot dominerer.

Illustrasjonen i figur 4 gir ei forenkla, visuell framstilling av risikoen for utfall i ulike delar av ekomnettet, uttrykt som sannsyn for og konsekvens av ulike uønska hendingar. Figuren viser òg korleis trafikkvolumet aukar frå aksessnett til transportnett. I tråd med dette har utfall i regional- og landsnett (transportnett) større konsekvensar enn utfall i aksessnett, men sannsynet for slike hendingar er lågare grunna høgare robustheit. Dette kjem mellom anna av ein annan nettverkstopologi og fleire risikoreduserande tiltak.



Figur 4: Risiko for utfall i ulike ekomnett

Dei mest vanlege årsakene til utfall i ekomnetta i Noreg er ein kombinasjon av naturhendingar og menneskelege aktivitetar, slik som graving og planlagt arbeid i netta. Sjølv om desse årsakene står for ein vesentleg del av dei rapporterte hendingane, er det viktig å vere merksam på at det finst fleire andre faktorar som kan påverke stabiliteten og sikkerheita i nett og tenester.

Dei følgjande kapitla gir ein breiare gjennomgang av ytterlegare risikomoment, som den sikkerheitspolitiske situasjonen, fysisk sabotasje, personellsikring, verdikjeder, cyber-hendingar, planlagt arbeid i netta, naturhendingar og satellittbaserte tjenestar. Dette gir ei djupare forståing av dei samla utfordringane ekomnetta står overfor.

2.2 STATLEGE TRUSLAR

Den sikkerheitspolitiske utviklinga fører til auka risiko òg for ekomsektoren. Det er mogleg å hente inn informasjon om norsk ekominfrastruktur gjennom opne kjelder, cyberoperasjonar eller fysiske observasjonar. Strategiske oppkjøp kan òg nyttast for å få tilgang til sensitiv informasjon om kritisk infrastruktur. Målet med slik kartlegging er ofte å skaffe oversikt over verdiar og kvar ein er sårbar.

Kinesisk etterretningsaktivitet mot Noreg skjer i hovudsak i cyberdomenet, der informasjon blir henta ut og kombinert med data frå ulike kjelder. Slik kan ein til dømes identifisere potensielle menneskelege kjelder for vidare etterretningsinnhenting[12].

NSM peikar i si opne trusselvurdering *Risiko 2024*[13] på at dronar kan nyttast til både etterretning, sabotasje og terrorverksemd. I *Risiko 2025*[14] blir det understreka at dronar kan vere utstyrte med sensorar som kan brukast til avlytting, overvaking og sporing. Krigen i Ukraina har vist at kommersielt tilgjengelege dronar blir nytta til etterretning, og at dei enkelt kan modifiserast til angrepsdronar.

Fysisk sabotasje
PST åtvarar mot auka risiko for sabotasjeangrep mot Noreg. I nabolandet vårt, Sverige, etterforskar politiet sabotasje mot ekom-infrastruktur langs E22 på austkysten våren 2025. Stockholm har vore utsett for fleire titals sabotasjeaksjonar der fiber og mobilmaster har vore målet.

Styresmakter og verksemder bør ta dette på alvor og setje i verk førebyggjande tiltak for å sikre verdiar og redusere sårbarheiter. Systematisk arbeid med sikring, etablering av reserveløysingar og god reparasjonsberedskap er viktigare enn nokon gong. Sabotasje kan vere knytt til Noregs støtte til Ukraina, og Etterretningstenesta peikar i *Fokus 2025*[15] på at Russland kan rette aksjonar mot både våpenleveransar og kritisk infrastruktur dersom krigen utviklar seg i Ukrainas favør.

I *Fokus 2024* skriv Etterretningstenesta at Russland over fleire år har kartlagt norsk olje- og gassinfrastruktur. Vidare viser *Fokus 2025* til at Russland utviklar militære evner til å rekognosere og sabotere undervassmål i Vesten. Målet er å kunne true kritisk infrastruktur under vatn i ein konflikt. Trusselbiletet omfattar særleg undervassinfrastruktur som fiberkablar og energirøyr, som representerer ei strategisk sårbarheit for Noreg.

Sjøkablar har den siste tida fått mykje merksemd etter fleire hendingar i Austersjøen. På verdsbasis skjer det mellom 150 og 200 kabelbrot kvart år, og dei fleste skuldast fiskereiskap, ankring eller dregging. Etterretningstenesta har understreka at det ikkje finst bevis for at hendingane i Austersjøen skuldast noko anna enn uhell, og sjefen for tenesta har åtvara mot «sjølvskremming». Dårleg sjømannskap og teknisk svikt er nemnde som moglege årsaker.

Personellsikkerheit og innsidetruslar

Auka trussel om sabotasje inneber også at det er ein auka sjanse for at innbyggjarar, styresmakter og ulike organisasjonar står utan ekom. I desse tilfella bør folk ha ein møtestad i kommunen der dei veit at dei kan snakke med nokon og eventuelt få varsla om naudsituasjonar. Totalberedskapsmeldinga omtalar dette som sikkerheitspunkt. Nkom er kjend med utfordringa kommunane har relatert til desse sikkerheitspunkta, og det er mange spørsmål knytt til organiseringa og kommunikasjonen ut for lokasjonar og bruk av desse. Nkom meiner likevel at dette er eit viktig arbeid som kommunane må prioritere, og ha planar klare for eventuelle langvarige ekomutfall i sin kommune.

Tilbydarar av samfunnskritiske nett og tenester, samt datasenteroperatørar som leverer samlokasjonstenester, er attraktive mål for etterretning og innsideverksemd. Slike aktørar kan bli kartlagde for å identifisere kvar ein er sårbar og angrepsflater i infrastruktur og tenester, som seinare kan bli utnytta i ein tilspissa sikkerheitspolitisk situasjon. Eit bortfall av desse kritiske funksjonane kan få store og tverrsektorielle konsekvensar for samfunnet.

Derfor er det viktig at tilbydarar og datasenteroperatørar arbeider systematisk med sikkerheitsstyring og tiltak som reduserer innsiderisiko. Dette handlar ikkje berre om kunnskap, men òg om å utvikle ein sterk sikkerheitskultur og å sikre at dei tilsette er tilfredse. Ein god organisasjonskultur kan gjere ein mindre sårbar for både medviten og ikkje medviten innsideverksemd. Erfaringar frå Sikkerhetskonferansen 2025 understreka at tiltak som open kommunikasjon, god leiing, og oppfølging av arbeidsmiljø er vel så viktige som formelle kontrollmekanismar.

Internasjonalt ser vi ein auke i innside-problematikk. I amerikanske forvaltingsorgan er det uttrykt uro for at masseoppsseiingar kan føre til større innsiderisiko, ettersom misnøgde eller økonomisk pressa tidlegare tilsette kan vere meir mottakelege for rekrutteringsforsøk.

Det finst fleire døme frå vestlege land i 2024 på innsideverksemd, forsøk eller mistanke om slik aktivitet. Sidan invasjonen av Ukraina i 2022 er fleire europeiske borgarar arresterte og tiltalt for etterretningsaktivitet på vegner av russiske tenester. Nokre har handla under press mot seg sjølv eller familien, men i mange tilfelle har økonomiske insentiv vore motivasjonen. Personar med familietilknyting eller annan nær relasjon til Russland er særleg utsette for rekrutteringsforsøk[16].

[12] Etterretningstjenesten – Fokus 2024
[13] Risiko 2024 - Nasjonal sikkerhetsmyndighet
[14] Risiko 2025 - Nasjonal sikkerhetsmyndighet
[15] Etteretningstjenesten – Fokus 2025
[16] NTV 2024 Nasjonal Trusselvurdering 2024 NTV 2024

2.2.1 VURDERINGAR OG RISIKOREDUSERANDE TILTAK

I Noreg har sjøkabelaktørar og styresmakter nyleg etablert Norsk Sjøkabelforening, som har sikkerheit for sjøkablar som hovudføremål. Slike samarbeidskonstellasjonar, der styresmakter og verksemder møtast for å dele informasjon og samarbeide om sikkerheit, er ein styrke og kan gi betre effekt i arbeidet med sikring av sjøkablar.

Det er særleg utfordrande å verne seg mot innsidarar, då dei kan opptre både med og utan medvit. Sektoren er dessutan avhengig av mykje utanlandsk personell, der prosessen med sikkerheitsklarering tek lang tid. Nkom vurderer at bruk av innsidarar hos ekomtilbydarar og datasenter representerer ein reell risiko for kartlegging, etterretning og mogleg gjennomføring av sabotasje- eller cyberangrep. I denne samanhengen er det viktig å få opp farten på behandlinga av sikkerheits- og tilgangsklareringar.

For å redusere innsiderisiko bør verksemdene arbeide systematisk med sikkerheitskultur, open kommunikasjon og oppfølging av tilsette. Tiltak som å fremje trivsel, god leiing og medviten haldning til sikkerheit kan bidra til å gjere organisasjonane mindre sårbare, og dermed styrkje det samla vernet mot innsideaktivitet.

2.3 VERDI- OG LEVERANDØRKJEDER

Verdi- og leverandørkjeder kan vere komplekse og uoversiktlege. Manglande kontroll og oversikt gjer verdikjeder sårbare for påverknad frå trusselaktørar. Utnytting av denne sårbarheita kan vere ein metode for å tileigne seg informasjon, påverke drift og styring, eller i verste fall ta kontroll over system og infrastruktur.

Sårbarheiter i verdikjeder er løfta fram som eit sentralt tema både i Totalberedskapsmeldinga[17] og i rapporten frå Totalberedskapskommisjonen[18]. Næringslivet har fått ei stadig meir framståande rolle i totalforsvaret, sidan mykje av infrastrukturen, varene og tenestene er i privat eige. Dette gjeld òg for ekomsektoren.

Å vere avhengig av spesialisert maskinvare og programvare

Det kan vere utfordrande å skaffe reservedelar til eldre system dersom dei ikkje finst på lager. Mange tilbydarar har derfor inngått samarbeid med aktørar som nyttar liknande utstyr, noko som bidreg til å styrkje tilgangen på reservedelar. Det kan òg vere risiko knytt til at gamalt («legacy») utstyr ikkje kan oppgraderast med nye versjonar av programvare og fastvare, noko som gjer dei meir sårbare for sikkerheitstruande hendingar.

Leveransar av teknologikomponentar, spesielt avansert elektronikk, blir rekna som sårbare i globale verdikjeder. Produksjonen er ofte konsentrert i nokre få geografiske område, noko

som gjer leveransane utsette for påverknad frå geopolitisk uro og internasjonale konfliktar. Slike hendingar kan føre til forstyrringar i forsyningslinjene og påverke tilgangen på kritiske komponentar.

Prinsippet om «just-in-time»-leveransar, som betyr at varer skal bli levert akkurat når dei trengst, blir utfordra når det oppstår uventa forstyrringar i dei globale leveransane. Dette kan få konsekvensar for både produksjon, drift og beredskap i sektorar som er avhengige av stabil tilgang på spesialisert utstyr.

Høg grad av spesialisering og stort kapitalbehov for å setje i gang produksjon kan føre til at få leverandørar tilbyr kritiske system og utstyr til tilbydarar av ekomnett. Dette gjer at tilbydarane sine verdi- og leverandørkjeder kan ha låg grad av mangfald og vere utsette for påverknad. I det digitale domenet kan det at ein er logisk sårbar og feil i programvare råke fleire tilbydarar samtidig, noko som aukar konsekvenspotensialet ved sikkerheitstruande hendingar.

Det er òg ein aukande grad av virtualisering for å understøtte ekomnett, samt programvare-definert styring av ekomnetta. Desse teknologiane blir ofte leverte av IT-selskap og kan føre til ein blir meir avhengig av tredjepartar for drift og støtte. Dette kan endre risikobiletet og introdusere at ein blir sårbar på nye måtar når nye aktørar blir ein del av leveransekjeda. I tilbydarane sitt arbeid med sikkerheitsstyring og beredskapsplanlegging må ein ta høgde for dette.

Tilgang til teknisk kompetanse
Tilgang på kompetent personell er ein avgjerande faktor for drift og tenesteproduksjon i ekomsektoren. I løpet av få år kan det oppstå ein stor mangel på kvalifisert arbeidskraft innan tekniske fagområde, som til dømes telekommunikasjon. Tilsvarande utfordringar blir også rapporterte frå internasjonale aktørar.

Konsentrasjonsrisiko
Med konsentrasjonsrisiko meiner ein at fleire tilbydarar har kritisk utstyr eller verdiar samla på eit avgrensa geografisk område, til dømes i eit datasenter. Dette kan vere utstyr som blir brukt til drift og styring av ekomnett, tenesteproduksjon og trafikkutveksling mellom ekomnett. Risikoen aukar dersom andre sektorar har kritiske verdiar innanfor det same området – til dømes maskinvare i datasenter som køyrer IT-system med ulik grad av kritikalitet. Kor verdifull og sårbar ein lokasjon (som eit datasenter) er, heng tett saman med kundar og sektorar som er avhengige av lokasjonen og maskinvaren som finst der.

Frå 1. januar 2025 er både kommersielle og enkelte interne datasenter underlagt registreringsplikt og krav til sikkerheit og beredskap etter ny ekomlov. Dette inneber at datasenteroperatørar må oppfylle ei rekke plikter knytt til sikkerheit og varsling. Slike krav er særleg relevante ved samlokalisering, der konsentrasjon av kritisk utstyr og verdiar kan medføre auka risiko for at ein blir meir sårbar og påverknad. Ved samlokalisering i kommersielle datasenter kan det vere krevjande for kundar, inkludert ekomtilbydarar, å vite kven som har innplassering i same lokale, eller kva personell som har tilgang.

[17] Totalberedskapsmeldingen: Forberedt på krise og krig - regjeringen.no
[18] NOU 2023: 17 - regjeringen.no

2.3.1 VURDERINGAR OG RISIKOREDUSERANDE TILTAK

Nkom ser alvorleg på risikoen for redusert tilgang til kritisk utstyr og utanlandsk arbeidskraft som følgje av ein forverra sikkerheitspolitisk situasjon globalt. Handel og produksjon av strategiske ressursar blir i aukande grad brukt som pressmiddel i rivalisering mellom statar.

Tilbydarar bør ha god oversikt over korleis verdikjeder og leverandørkjeder er knytt saman for å kunne identifisere dei viktigaste faktorane som er nødvendige for drift og tenesteproduksjon. Dette gjeld både for prioriterte områder og generell infrastruktur. Desse kjedene fins både innanlands og utanlands, og det er viktig å ha innsikt i kven ein samarbeider med og er avhengig av.

Den nye reguleringa for datasenter i samsvar med ekomlova tok til å gjelde 1. januar 2025. Reguleringa omfattar både kommersielle datasenter og enkelte interne datasenter med eit straumforbruk over 0,5 megawatt. Alle datasenter som blei omfatta hadde registreringsplikt hos Nkom innan 1. juli 2025. Datasenteroperatørane må oppfylle krav til forsvarleg sikring og beredskap, med særleg fokus på sikring og varsling. Risikoreduserande tiltak inkluderer utvikling og bruk av sikre protokollar, etablering av strenge kontrollmekanismar for tilgang, og gjennomføring av grundige risikovurderingar.

2.4 PLANLAGT ARBEID I NETTET

Programvare, maskinvare og hjelpeteknisk utstyr treng regelmessige oppgraderingar og vedlikehald. Av og til kan det oppstå problem under planlagt arbeid som gjer at tenestene blir mindre tilgjengelege.

Feil i hjelpeteknisk utstyr og maskinvare kan spreie seg til høgare nettverkslag[7] og påverke logiske funksjonar, og i siste instans tilgang til tenestene i mobil- og fastnettet. Det er derfor viktig å ha tilstrekkeleg redundans både i hjelpeteknisk utstyr, maskinvare og nettverks¬element.

Det er ein aukande kompleksitet i oppbygginga av fastnett og mobilnett, blant anna fordi tradisjonelle IT-system blir meir brukt til å støtte drift og tenesteproduksjon. Eit kjernenett kan til dømes bestå av nettelement som er levert av fleire forskjellige leverandørar. Den kompliserte samansetninga av ulike system og nettelement frå forskjellige leverandørar kan gjere det vanskelegare å ha oversikt over kva som er avhengig av kva, og sjå konsekvensar ved endringar. Det at fleire system er gjensidig avhengige av kvarandre og tett kopling mellom nettelement og grensesnitt mellom desse, gjer at feiltilstandar raskt kan spreie seg til større delar av systema.

Mobilnett er svært komplekse system som er avhengige av konsistens og synkronisering på tvers av nettelement og instansar av desse. Dette gjeld både i kjernenett og i logikken i radionettet, samt i tilknytingane mellom desse.

[7] Jamfør OSI-modellen, som består av det fysiske laget (fiber mv.), data link-laget (ethernet mv.), nettverkslaget (IP), transport (TCP, UDP), sesjonslaget (synkronisering, til/fra port, API mv.), presentasjonslaget (syntax samt ulike protokollar og format som SSL, SSH, IMAP og JPEG), og applikasjonslaget (HTTP, FTP, DNS mv.)

HENDELSESBOKS

I løpet av hausten 2024 har det ved fire tilfelle vore uønska hendingar som har påverka naudmeldingstenesta.

Torsdag 29. august 2024 vart Nkom, gjennom redaksjonell media, gjort merksam på at det var problem med politiet sitt naudnummer 112. Politiet informerte media om at politidistrikta ikkje kunne ta imot meldingar frå publikum på naudnummeret. Gjeldande samtalar vart opplevde som stumme oppringingar. Feilen oppstod i samband med ei planlagt oppgradering av ei tenesteplattform og ramma mobiloppringingar som vart gjort over 4G til naudnummeret 112 i heile landet i ein tidsperiode på 2 timar og 20 minutt.

Måndag 16. september 2024 feila tidvis mobiloppringing over 4G i verksemda sitt nett mot naudnummer 110 og 112 i heile landet. Oppringingane vart, som ved hendinga 29. august, opplevde som stumme oppringingar av operatørane på naudmeldesentralane. For oppringing til naudnummer 113 var feilen berre synleg gjennom feil nummervising for enkelte oppringingar. Feilsituasjonen vart utløyst av problem knytt til kommunikasjon mellom nettverkselement. Dette førte til at prosessar i ei tenesteplattform hengde seg opp, og viktig signalering dermed ikkje vart tolka korrekt, noko som påverka talemeldinga. Feilen varte i 56 minutt.

Torsdag 17.-18. oktober 2024 vart oppringing frå verksemda sine abonnentar til naudnummer 110, 112 og 113 ikkje sett til korrekt geografisk naudmeldesentral. Samtalene vart i staden ruta til alternativ svarstad, som var naudmeldesentralene i Oslo. Dette fungerte for 110 og 112, men oppringingsoppsett tok noko lenger tid. For 113 vart oppringing ruta til feil nummer, som medførte at innringar mottok ei talemelding med beskjed om at nummeret ikkje var i bruk. Dette skuldast ein organisatorisk feil ved at nummeret til naudnummeret 113 ikkje vart endra som det skulle. Feilen varte i 3 timar og 24 minutt.

Onsdag 13. november 2024 vart det utført vedlikehaldsarbeid på ei av verksemda sine lokasjonar. I samband med vedlikehaldet vart det gjort ein feil som medførte at utstyr mista tilgang til straum og derfor slo seg av. Normalt ville ikkje dette ha fått anna enn lokale konsekvensar, men ein konfigurasjonsfeil medførte at dei redundante løysingane ikkje fungerte slik dei vart tenkt. Etter ei stund vart feilen retta, men då hadde allereie fleire tenester blitt påverka. Dette gjaldt mellom anna naudnummer-tenester, mobil tale og data, oppringing til diverse spesialnummer og fast trådlaust breiband.

2.4.1 VURDERINGAR OG RISIKOREDUSERANDE TILTAK

Nkom ser at det er utfordrande å ha full oversikt over risiko når planlagt arbeid er så komplekst. Konfigurasjonsendringar kan få uventa ringverknader som først blir synlege når endringane er utført, og då kan det vere nødvendig å rulle tilbake endringane. Det er derfor viktig å ha gode rutinar for å vurdere risiko knytt til planlagt arbeid, samt å ha tilstrekkelege rutinar for å rulle tilbake endringar ved behov for å gjenopprette den opphavlege konfigurasjonen.

Nkom gjennomfører jamnlege tilsyn med tilbydarar etter feil ved planlagt arbeid, og resultat frå tilsynene viser at manglande eller feilslåtte risikovurderingar ofte går igjen. Dei fleste hendingane har sin bakgrunn i organisatorisk eller menneskeleg svikt, og ikkje i teknisk svikt som sådan. Andre årsaker er komplekse leverandørkjeder med fragmentert ansvar og manglande heilskaplege risikovurderingar.

Ved utsetting av IT-system og bruk av tredjepartar for levering av nettverksfunksjonar, er det viktig med ei risikovurdering for å vurdere betydninga for driftsstabilitet, kontroll og sikkerheit. Det bør også gjerast tilstrekkeleg testing og verifikasjon i isolerte miljø før endringar blir sett i produksjon.

Det er også viktig å prioritere arbeidet med å analysere varsel frå kontrollsystem. Ved mange av dei store sikkerheitshendingane har ein i ettertid sett at kontrollsystem tidleg har varsla på avvik, uten at dette har blitt fanga opp. Dersom ein hadde fanga opp desse varsla tidleg kunne ein ha oppdaga og dermed kanskje avverga angrep.

For å unngå uønska hendingar ved planlagt arbeid i elektroniske kommunikasjonsnett, må verksemder sette i verk systematiske og målretta tiltak.

Følgjande tiltak medverkar til å redusere risiko og sikre verna gjennomføring:

- Alt planlagt arbeid må følgje etablerte prosedyrar og sikkerheitskrav for å unngå utilsikta driftsforstyrringar.
- Før ein set i gang arbeid, skal det gjennomførast ei grundig risikovurdering for å identifisere mogelege konsekvensar og nødvendige risikoreduserande tiltak.
- Endringar må testast grundig før implementering, og det bør gjennomførast evalueringar og revisjonar av arbeidet for å lære av eventuelle feil.
- Risiko- og sårbarheitsvurderingar må vere oppdaterte og dekke alle relevante aspekt av arbeidet.
- Det må vere fungerande reserveløysingar for kritiske tenester, slik at ein feil ikkje fører til omfattande tenesteutfall.
- Underleverandørar må jamleg reviderast for å sikre at dei oppfyller krava til sikkerheit, beredskap og kvalitet.
- Det må vere tydelege rutinar for rask og presis varsling til relevante styresmakter og interessentar dersom det oppstår avvik under planlagt arbeid.
- Bruk av styringssystem og system for kvalitetssikring i samband med planlagt arbeid.
- Sidemannskontroll ved endringar som har eit stort konsekvenspotensial.
- Rutinar for tilbakerulling av endringar.
- Test av tilbakerulling.
- Gjennomføring av planlagt arbeid til tider på døgnet der konsekvensen ved feil vil bli mindre.
- Å arbeide for best mogleg systemkunnskap for å forstå korleis konfigurasjonsendringar kan påverke systemet og korleis feiltilstandar kan oppstå ved konfigurasjon.

2.5 CYBERDOMENET

I cyberdomenet er det utfordrande å halde oversikt over trusselbiletet, fordi cyberangrep ofte ikkje diskriminerer eller nødvendigvis er retta mot eit konkret selskap, sektor eller stat. Trusselaktørar kan utnytte ei rekke angrepsflater basert på kvar ein er sårbar menneskeleg, organisatorisk og teknisk i varierande grad. Dette blir vanlegvis gjort for å få tilgang til, samt for å skade og/eller påverke IT-system.

Det er viktig å prioritere arbeidet med å analysere varsel frå kontrollsystem. Ved fleire store sikkerheitshendingar har ein i ettertid sett at kontrollsystem tidleg varsla om avvik, utan at dette blei fanga opp. Dersom slike varsel hadde blitt oppdaga tidlegare, kunne angrepa kanskje vore oppdaga og i beste fall avverga.

Trusselbilete og trendar

Cybertruslar mot ekomsektoren kjem frå ei blanding av økonomisk motiverte kriminelle aktørar og statlege aktørar frå land som Russland, Kina, Nord-Korea og Iran. Særleg Russland og Kina har avanserte kapasitetar og er venta å stå bak ein stor del av dei mest alvorlege operasjonane mot Noreg. Desse aktørane nyttar avanserte teknikkar som utnytting av nulldagssårbarheiter, verdikjedeangrep og "Living Off the Land"-metodar, der dei opererer i kompromitterte system utan å etterlate spor. Ein aukande tendens er bruk av proxy-aktørar, der cyberkriminelle eller kommersielle teknologiselskap utfører angrep på vegner av statlege aktørar, noko som gjer attribusjon og respons meir utfordrande[12].

Nye måtar å organisere og konfigurere leveransen av tenester på, gjer den meir effektiv, meir skalerbar og gir auka kvalitet. Men dette fører også til at det blir meir komplekst og sårbart. Døme på nye måtar er bruk av kunstig intelligens (KI) til å konfigurere og overvake ekomnett. KI kan bidra til at ein raskare oppdagar anomaliar og til generell effektivisering av nettverksovervaking. Samtidig fører teknologien til mogleg "svart-boks"-problematikk, då ein ikkje nødvendigvis kan stole på datasettet som den kunstige intelligensen er basert på.

Bruken av KI har auka suksessraten på økonomisk motiverte cyberangrep. Svært sofistikerte spearphishing-operasjonar kan bli sende ut i stort omfang med høgare suksessrate, sidan angrepa er betre tilpassa det enkelte offer.

Cyberangrep utviklar seg raskt med aukande kompleksitet og profesjonalisering. Åra 2023 og 2024 var rekordår for internasjonale cyberangrep, og ekomsektoren var ikkje eit unntak. Sentrale leverandørar av nettverkstenester har rapportert at dei har dempa angrep mot tenesteavbrudd i ein skala som aldri har vore observert før[19].

Ifølgje Kripos sin rapport "Cyberkriminalitet 2025[20]", er trenden at kriminelle i aukande grad samarbeider på tvers av landegrenser, utnyttar kunstig intelligens og brukar digital infrastruktur for å skjule identitet og transaksjonar. Cyberkriminelle brukar stadig meir avanserte teknologiar, som djupforfalskingar og automatiserte KI-verktøy, til svindel og manipulasjon. I tillegg aukar bruken av løysepengevirus-angrep, der utpressing utan nødvendigvis å kryptere filer blir meir vanleg. Kripos ventar at når ein er sårbar vil det bli utnytta raskare, og at kriminelle tenester blir lettare tilgjengeleg på det mørke nettet. Det er meir vanleg at cyberkriminalitet er tettare knytt til annan organisert kriminalitet. Dette utfordrar politiet og sikkerheitsstyresmakter i deira arbeid med å motvirke truslane.

Talet på registrerte datalekkasjeoppføringar knytt til EU sin digitale infrastruktur auka frå 9 til 11 i rapporteringsperioden november-desember

2024. For andre halvår 2024 vart det registrert ein markant auke frå 21 oppføringar i første halvår til 30, noko som tilsvarar ein auke på 43 %. I same periode utgjorde EU-baserte verksemder 22 % av dei globale datalekkasjeoppføringane innan digital infrastruktur[21].

Døme på cyberangrep mot ekom og digital infrastruktur

Her følgjer eit utval viktige cyberhendingar som utgjorde sikkerheitstruslar mot ekomsektoren i forskjellige land i 2023 og 2024 (Tabell 1). Hendingane omfatta hovudsakleg brot på konfidensialitet og tilgjenge. Dei hadde sin bakgrunn i sårbare både menneskelege, organisatoriske og tekniske årsaker. Trusselaktørane bak hendingane inkluderte vinnings-kriminelle, statlege aktørar og hacktivistar som opererte relativt sjølvstendig eller med laus tilknyting til statar. Informasjonen er henta frå opne kjelder.

Sjå tabellen på side 27.

Geopolitikk og cyberdomenet

Endringstendenser i det geopolitiske landskapet har betydning for cyberdomenet. Kina innførte i 2017 ei etterretningslov som pålegg enkeltpersonar og verksemder å dele informasjon med kinesiske styresmakter. Vidare tok ei cybersikkerheitslov til å gjelde i Kina i 2021. Lova pålegg produsentar av nettverksutstyr å rapportere sårbarheiter som blir oppdaga til kinesiske styresmakter. Lova forbyr offentleggjering av kvar ein er sårbar utan godkjenning frå kinesiske styresmakter. Slik regulering kan gi den kinesiske staten meir handlingsrom til å utnytte nye angrepsflater, og medføre at andre statar blir meir sårbare for cyberangrep.

I samband med krigen i Ukraina og konflikten mellom Israel og Hamas har det mellom anna vore utført tenestenektangrep, destruktive angrep og BGP-kapring mot ekomnett[22]. Etter hendingane i 2022 vart det innført tiltak som gjer BGP-kapring vanskelegare. I krigen i Ukraina har det også skjedd rettsstridig overtaking. Russland har mellom anna tatt over, i staden for å øydeleggje ekominfrastruktur i Aust-Ukraina.

Ei gruppering som støttar Russland si krigføring i Ukraina, sette sommaren 2024 fram truslar mot og utførte tenestenektangrep mot Nkom og fleire norske ekomtilbydarar. Truslane og angrepa var grunngitt i at regjeringa ville overføre seks F16 jagarfly til Ukraina, og at norske styresmakter var russofobiske. Dette viser at Noreg sitt bidrag til forsvaret av Ukraina også gjer ekomsektoren til eit mogleg mål for cyberangrep.

Ekomnett har også blitt brukt til kampanjar med desinformasjon og sosial manipulering for å kontrollere narrativ, spreie politiske bodskap og ha innverknad på folkeopinionen og beslutningstakarar i samband med fleire konfliktar.

---

[12] Etterretningstjenesten – Fokus 2024

[19] Sjå til dømes Cloudflare Thwarts Largest-Ever 3.8 Tbps DDoS Attack Targeting Global Sectors og 2024 DDoS Attack Trends | F5 Labs

[20] Cyberkriminalitet 2025, Politiet sin årlege rapport om cyberretta og cyberstøtta kriminalitet

[21] ENISA (EU), SA report, Digital Infrastructure sector 2025

[22] BGP-kapring vil seie at trafikk som eigentlig skal til ein sluttbrukar, blir ruta om og sendt til ein vondsinna aktør.

Tidspunkt	Hending	Skildring
September 2023	Lekkasje av Lyca Mobile kundedata	Eit datainnbrudd førte til at mange av kundane sine data hamna på gale vegar.
Oktober 2023	Lekkasje av Xfinity kundedata	Ei løysing levert av Citrix var sårbar og førte til at kundeinformasjon, brukarnamn og passord hamna på gale vegar. Lekkasjen omfatta 36 millionar kundar til breidbandstilbydaren Xfinity.
Desember 2023	Angrep mot KyivStar	Destruktivt angrep mot KyivStar sitt kjernenett i samband med krigen i Ukraina. Heile kjernenettet vart sett ut av drift i ca. to veker med konsekvensar for 24 millionar kundar.
Januar 2024	Angrep mot Orange Spania	Kompromittering av innloggingsopplysningar til Orange sitt administrasjonssystem. Skadevare vart brukt til å endre kritisk nettverks-konfigurasjon, som førte til store problem med ruting i nettverket.
April 2024	Lekkasje av AT&T kundars metadata	Metadata til ein stor del av AT&T sine kundar blei lekka i samband med kompromittering av skytenesteleverandøren Snowflake.
Oktober 2024	Kompromittering av system for kommunikasjonskontroll	Eit system som amerikanske styresmakter brukte for kommunikasjonskontroll i ekomnett, vart påvist kompromittert av aktørar med tilknyting til den kinesiske staten (Salt Typhoon). Det totale omfanget er førebels ukjent.
Oktober 2024	Kompromittering av innloggingsopplysninger	Gjennom eit phishing-angrep fekk ein trusselaktør tak i innloggings¬opplysningane til ein tilsett hos ein norsk datasenteroperatør.
November 2024	Lekkasje av innloggings-opplysningar til administrasjonssystem	Påstand om at innloggingsopplysningar til Vodafone sitt administrasjonssystem for eSIM blei lekka på internett.
Januar 2025	Tenestenektangrep mot NTT Docomo.	Eit tenestenektangrep førte til omfattande utfall på mobil- og internettjenester som varte i 12 timar.

Tabell 1: Eit utval viktige cyberhendingar som utgjorde sikkerheitstruslar mot ekomsektoren i forskjellige land i 2023 og 2024

2.5.1 VURDERINGAR OG RISIKOREDUSERANDE TILTAK

Nkom vurderer at den dimensjonerende trusselen i cyberdomenet er avanserte økonomisk motiverte trusselaktørar og statlege trusselaktørar med tilhøyrande proxyar. Desse aktørane kan angripe både perifere og sentrale delar av ekomnett, noko som ein må ta omsyn til i arbeidet med sikkerheitsstyring og beredskapsplanlegging.

Robust arkitektur og overvaking blir stadig viktigare for ekomtilbydarane, fordi «tradisjonelle» tiltak ikkje er tilstrekkelege mot avanserte statlege trusselaktørar som utnytter nulldågssårbarheiter. Nkom vurderer at mellom anna følgjande risikoreduserande tiltak er viktige med omsyn til dette:

- Redusere unødvendig eksponering mot Internett.
- Innføre prinsipp som Zero Trust og Least Privilege for tilgangs- og rettigheitsstyring.
- Ha tilstrekkeleg overvaking av uventa endringar (anomalideteksjon).

Risikovurderingar og tillit er viktig ved tenesteutsetting av drift, administrasjon og logisk infrastruktur. Det er nødvendig å gjere vurderingar av verdi og kva som er avgengig av kva, for å vite kva for tenester som kan setjast ut. Dette inkluderer tilstrekkelege vurderingar av kva tenesteutsetting betyr for kontroll over utstyr og IT-system, samt mogelege angrepsflater.

Nkom tilrår generelt å sjå til NSM sine grunnprinsipp for IKT-sikkerheit, samt NIST og CISA sine retningslinjer for IKT-sikkerheit. Standardar som ISO27000-serien og IEC 62443 er tillrådd brukt som underlag til arbeid med IT-sikkerheitsstyring og styrking av nettverk. CISA, NSA og FBI har i samband med Volt Typhoon og kompromitteringa av fleire amerikanske ekomtilbydarar gitt ut eit skriv med tiltak for betre grunnsikring og auka deteksjonsevne[23].

[23] Cybersecurity Advisory – PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Alert Code: AA24-038A.

Foto: Anders Martinsen

2.6 SVINDEL

Digital svindel er eit samfunnsproblem. Det totale svindeltapet auka med 51 prosent frå 2022 til 929 millionar kroner i 2023, ifølgje tal frå Finanstilsynet[24]. I 2024 var svindeltapet på over 1,2 milliardar kroner.

Ein stor del av svindelen skjer i finanssektoren, og det samla tapet for svindel med til dømes kontooverføringar og betalingskort er stadig aukande. Finanstilsynet rapporterer i sin svindel-statistikk for 2024 at tapa auka frå 522 millionar kroner i andre halvår 2023 til 607 millionar kroner i første halvår 2024. På den andre sida har tilbydarar av betalingstenester hindra svindel for 1 341 millionar kroner i første halvår 2024.

I ekomsektoren er telefonsvindel eit kjent problem. Ved mange av svindeltilfella blir spoofa telefonnummer (telefonnummeret ditt blir lånt av andre med uærlege hensikter) og/eller SMS med svindel-lenkje eller instruksjonar om å laste ned appar brukt i kommunikasjon med offeret. Offeret blir bedt om å oppgi sensitiv informasjon som koder eller passord og gir vidare svindlaren tilgang til mobilbank og liknande tenester.

Dei siste åra er det årleg meldt over 30 000 bedrageri til politiet, og ein går utifrå at mørketala er store. Politiet har no etablert moglegheit for digital melding av svindel, noko som er venta å føre til ein auke i talet på meldingar.

Nkom ser at svindlarane finn smutthol i dei norske digitale skjolda og skiftar raskt modus etter kvart som nye tiltak blir innført. Til dømes auka trafikken betydeleg inn til Noreg frå danske spoofa nummer kort tid etter at det koordinerte roaming proxy skjoldet vart innført i november 2024. Dette har resultert i at 76 millionar svindelanrop frå norske mobilnummer er blitt blokkerte frå slutten av november 2024 til august 2025.

[24] Finanstilsynets svindelstatistikk: Svindel og svindelstatistikk - Finanstilsynet.no

2.6.1 VURDERINGAR OG RISIKOREDUSERENDE TILTAK

Svindel har både økonomiske og psykologiske konsekvensar for den fornærma parten, og svindeltrykket kan utfordre tilliten til ekomtenester. Konsekvensane av redusert tillit til ekomtenester kan vere alvorlege i dagens samfunn der digitalisering er så integrert i dagleglivet. Effektiviteten i både offentleg og privat sektor kan bli svekka dersom innbyggjarar vel alternative løysingar til fordel for meir tidkrevjande alternativ. Redusert bruk av automatiserte tenester kan medføre auka driftskostnadar, særskilt innan helse og velferdssektoren. Dette kan føre til svekka sikring av pasientar og meir press på tradisjonelle tenester. I tillegg kan redusert tillitt føre til digital ekskludering, der delar av innbyggjarane mister tilgang til viktige tenester og informasjon.

Nkom etablerte i 2023, i samarbeid med Økokrim, ei nasjonal ekspertgruppe mot ekomsvindel. Her deltek i tillegg til Nkom og Økokrim, mobilnetteigarar, Nasjonal referansedatabase og observatørar frå NSM, FinansNorge, Næringslivets sikkerhetsråd, BankID og DigDir. Ein effekt av dette samarbeidet er at Noreg implementerte i november 2024 eit koordinert digitalt skjold, ein form for «grensekontroll», for å beskytte mot misbruk av mobilnummer, eller meir konkret; urettmessig manipulasjon eller spoofing av norske mobilnummerressursar. Systemet vart utvikla av mobilnetteigarar under prosjektleiing av Nasjonal Referansedatabase og filtrerer i sanntid omfattande mengder svindeltrafikk som prøver å kome inn i Noreg. Dei første ni månadane av drift vart 76 millionar oppringingar blokkert. På toppen vart 500 oppringingar blokkert i sekundet.

Kombinert med fastnettnummer-blokkering som har vore i drift sidan november 2022, har Noreg per no eit relativt effektivt vern mot misbruk av norske nummer. Resultatet gir auka tillit til norske nummer, og svindlarar ser seg nøydde til å bruke utanlandske nummer.

Nkom har også vore sentral i etableringa av Global Informal Regulatory Antifraud Forum – GIRAF, som ein del av det globale initiativet «Restore Trust». Forumet jobbar med global harmonisering av antisvindeltiltak og byggjing av nettverk.

2.7 NATURHENDINGAR

Utilsikta hendingar som ekstremvêr fører ofte til utfall i ekomnett og kraftnett. Kraftutfall forplantar seg ofte i ekomnetta på grunn av at ekom og kraft er gjensidig avhengige av kvarandre. Førekomst av ekstremvêr aukar i takt med klimaendringane, og dette er noko tilbydarane må ta høgde for i si risikostyring og beredskapsplanlegging.

Dei siste to åra har det vore fleire ekstremvêr som har ført til ekom- og kraftutfall. Ved samtidige straumutfall kan rettetida vere lengre fordi det må utbetrast på fleire stader og i fleire infrastrukturar (ekom og kraft) samtidig. Under ekstremvêr må HMS-omsyn ivaretakast når mannskap skal utretta feil, noko som kan føre til forsinkingar i rettetida.

Det har vore tre store stormar i 2024 og 2025 som resulterte i ekomutfall.

Oversiktsbilete frå Fagernes sentrum under ekstremværet Hans, tatt 11.08.23. Ekominfrastruktur var svært nærme å bli overfløymt på grunn av høg vassføring i vassdraget.

Kjelde: Webkamera, gjengitt i Avisa Valdres.


Foto: Gunstein Myhre

Ekstremvêr

Ifølgje meteorologisk institutt kan vi vente aukande temperaturar og nedbør i heile landet, og vi må vere førebudd på fleire episodar med kraftig styrtregn og sterk vind. Ekstremvêr vil også kunne ramme område som historisk sett ikkje har vore råka av mykje uvêr. Slike døme omfattar mellom anna ekstremvêret Hans i august 2023, Ingunn januar 2024 og Jakob i oktober 2024.

Under ekstremvêret Hans medførte ras og flaum fleire transmisjonsbrot som gjorde at ekom fall ut i fleire område. Det var spesielt Buskerud og Innlandet som blei hardast ramma under uvêret. Under ekstremvêret Ingunn førte kraftig vind til utfall av ekom. Hovudårsaka til utfall av ekom var tap av ekstern straumforsyning og fiberbrot. På eit tidspunkt var to av tre føringsvegar for Helsenett nede i Nord-Noreg.

I januar 2025 traff eit ekstremvêr Trøndelag og førte til eit av dei største regionsvise utfalla som har vore i ekomnett sidan ekstremvêret Dagmar i 2011. Den tekniske årsaka til utfallet var dobbelt transmisjonsbrot. Rotårsaka var at straumbrot og fiberbrot skjedde samtidig. I den verste perioden var det utfall på mellom 200 og 300 basestasjonar. Hendinga kastar lys over kor viktig det er å ha tilstrekkeleg reservestrøm og redundans i ekomnetta.

Oktober 2025 traff ekstremvêret Amy Noreg frå Trøndelag og sørover. Ekstremvêret førte til store straumbrot fleire stader og spesielt Telemark og Trøndelag blei hardt ramma. Dette førte til utfall av omkring 1200 basestasjonar for mobil og det var fleire kommunar som var heilt eller delvis ekomdøde. Hovudårsaka til ekomutfalla skuldast brot i straumforsyninga grunna lokale kraftutfall.

Det vil oftare kome periodar med kraftig nedbør på grunn av aukande temperaturar, og det er korttidsnedbøren som aukar mest. Intense nedbørsmengder, tung snø og snøsmelting på kort tid skapar dei største problema, som til dømes flaum, overvatn og overfløymingar i byar. Dette vil tidvis også føre til skadar på ekominfrastruktur.

Ekominfrastruktur er også sårbar for alle typar skred, og ofte går ekominfrastruktur av ulike årsaker gjennom område som er utsette for skred. Skred kan skade både nedgravne fiberkablar, fiberkablar som er trekte i luftspenn, og øydeleggje basestasjonar og nodehytter som er plasserte i rasområdet. I tillegg til å utgjere ein fare mot ekominfrastruktur, vil skred også utgjere ein potensiell fare for entreprenørar som skal feilrette i skredområdet. Dette kan medføre utfordringar i samband med rettearbeid i skredsoner.

”

Kommunikasjon under ekstremvêr: Erfaringar frå Ål kommune

«Under uvêra med flaum og ras i august 2023 vart det svært utfordrande å halde ved lag stabil og effektiv kommunikasjon i Ål kommune. Fleire faktorar bidrog til dette, og nedanfor følgjer ei samla framstilling av problema som oppstod i perioden 8.–11. august under «Hans», samt erfaringar frå uvêret med mykje regn helga 26.–27. august, kalla «Lille-Hans».

Begge føringane inn til sentralen vart brotne, noko som påverka dei tilknytte basestasjonane for både Telenor og Telia. Fastlinjer knytt til sentralen på Solhov gjekk ned, og dette førte til at mange innbyggjarar mista internettf. Unntaket var Ål kommune, som hadde internett via Hallingdal Kraftnett/Bruse, utanom Telenor sitt nett. Sidan mobilnetta til Telenor og Telia låg nede i store delar av Ål, vart det svært vanskeleg for innbyggjarane å få tilgang til kritisk informasjon frå kommunen. Mange sleit med å nå kommunen si nettside eller informasjon på plattformer som Facebook.

Prioritering av restkapasitet i telenettet, slik forskriftene tilseier, vart ikkje teken i bruk for å sikra kommunikasjon. Naudvarsel fungerte dårleg og nådde berre tilfeldig fram, ettersom mobilnettet var sterkt påverka av fiberbrot, og systemet manglar støtte for stadfesting av mottak. Kriseleiinga hadde heller ikkje oversikt over kven som hadde mottatt meldingane, og SMS med kvittering for mottak vart ikkje nytta.

Sikringsradioar (VHF) vart ikkje brukt under «Hans», men var sett i beredskap helga 26.–27. august. Det vart gitt tilgang til naudnett via lån frå Røde Kors, men med avgrensa tal på kanalar. Satellittelefonane vart ikkje sette opp under «Hans» grunna mangel på lading, men var operative under «Lille-Hans». Kriseleiinga i Ål hadde heller ikkje tilgang til reserveløysingar for datakommunikasjon uavhengig av fibernettet.

Det var uklart kven kriseleiinga skulle venda seg til for å få sett i verk reparasjon eller ivaretaking av samfunnskritisk infrastruktur. Det framstod heller ikkje som at Statsforvaltaren hadde innarbeidde prosedyrar for å handtera slike utfordringar på det tidspunktet. Telenor hadde ikkje klart definerte kontaktpunkt med døgnopen tilgang via e-post og telefon som kriseleiinga kunne nytta. Det vart heller ikkje kommunisert noko tydeleg vurderingsregime for alvorsgrad frå Telenor si side til kommunen og Statsforvaltaren, og det var uklart kven som har mynde til å prioritera tele- og datakommunikasjon når liner eller basestasjonar fell ut. Rutinar for løpande informasjon frå Telenor til kommunen og Statsforvaltaren, for risikovurdering i kriseleiinga, framstod ikkje som godt etablerte eller kommuniserte.

Problema og risikoen for liv og helse som oppstod når vital telekommunikasjon svikta i eit lokalsamfunn som Ål, vart svært tydelege under desse hendingane. Me brukte sikringsradioane for kontakt mellom mannskapa på reinseanlegget, teknisk avdeling og kriseleiinga, men dette fungerte ikkje tilfredsstillande. Veg og Park hadde nokre walkie talkie-einingar kjøpt på Biltema som vart brukt noko, men dei hadde ikkje særleg betre funksjonalitet enn sikringsradioane.

Foto: Anders Martinsen

Telekommunikasjonen generelt vart sterkt påverka av fiberbrot inn til Telenor sin sentral på Solhov, og me måtte bruke naudnettet. Mobilnettet var svært ustabilt – samtalar kom som oftast fram, men vart ofte brotne etter kort tid, og det var generelt vanskeleg å få gjennomført samtalar. Kva for mobilnett som var nede, varierte mellom ulike område, men store delar – og til tider heile – mobilnettet i området rundt Ål var ute av drift.

Bruse sitt fibernett var svært stabilt i sentrum og for kommunale bygg i perioden. Dette bidrog til at drifta i Ål kommune kunne haldast oppe utan store utfordringar. Me nytta fleire radiosamband, men desse var berre basert på direkte kommunikasjon mellom terminalane, noko som gav svært avgrensa rekkevidde og dermed låg nytteverdi.

Naudnettet var det einaste sambandet som verkeleg fungerte, og det vart nytta i stor grad under hendinga. Dei fleste etatar som deltok hadde med seg eige samband. I ettertid har me etablert ein plan for informasjonsspreiing når nett og telefon er nede. Denne inneber utpeiking av kjende møtepunkt rundt i bygda og bruk av ordonnansar som kan ha kommunikasjon til desse møtepunkta. Me har no tre oppmøtestader i kommunen ved EKOM-utfall.»

Beredskapsrådgivar, Ål kommune

Foto: Anders Martinsen

Brann

Skogbrannar i Noreg har historisk sett vore av mindre omfang. Skogbrannfaren er likevel stor i varmare periodar, og fleire europeiske land har opplevd svært store skogbrannar dei siste åra, mellom anna i Sverige sommaren 2018. Noreg opplevde også fleire skogbrannar dette året. Sidan 2018 har det ikkje vore liknande tilfelle i Noreg, men med eit varmare klima og aukande tørkeperiodar er dette eit sannsynleg framtidig scenario. Det er særleg sørlege og søraustlege delar av landet som er utsett for skogbrann.

Brann i sentralar og anlegg i ekominfrastrukturen kan skje, slik som då ein av Telenor sine sentralar brann i Lærdal i 2018. Ein brann i ekominfrastruktur og teknisk utstyr ved sentrale anlegg og knutepunkt kan bli kritisk dersom han ikkje vert oppdaga og sløkt raskt. Ekomtilbydarar er pålagt krav til brannsikring. Likevel er infrastrukturen sårbar for brann, spesielt under ekstreme vêrforhold som kan auke risikoen for skogbrannar.

Romvêr

Romvêr refererer til aktivitet i sola si atmosfære som kan påverke jorda. Dette inkluderer solstormar, solutbrot og masseutbrot av korona. Denne aktiviteten kan medføre store skadar på ekom. Solstormar kan slå ut kommunikasjonssystem, påverke satellittsystem og kraftnett. Solstorm-aktiviteten går statistisk sett i ein syklus på ein periode på om lag elleve år. På toppen av denne syklusen skjer solstormar i gjennomsnitt hyppigare og sterkare, men store enkelthendingar har skjedd i perioder med låg aktivitet. I 1989 traff ein solstorm jorda og lamma mellom anna krafttilførselen i Quebec i Canada.

2.7.1 VURDERINGAR OG RISIKOREDUSERANDE TILTAK

Det er ei utfordring at ekominfrastruktur ofte går gjennom område som er utsett for flaum og ras. I mange tilfelle går ekominfrastrukturen langs annan infrastruktur. Følgjeleg kan det vere krevjande og kostbart å legge om ekominfrastrukturen. Likevel vurderer Nkom at tilbydarane i ein del tilfelle kan gjennomføre tiltak for å bøte på risikoen knytt til naturhendingar. Desse inkluderer mellom anna:

- Heve nodehytter som huser aggregeringsnoder i transportnetta, som eit risikoreduserande tiltak mot flaum.
- Installere tilstrekkeleg brannsikring i nodehytter og noderom der det manglar.
- Sørgje for at kritiske fiberforsterkarar og aggregeringsnoder i transportnett er dimensjonerte med forsvarleg reservestraumkapasitet.
  Dette vil verke risikoreduserande mot omfattande regionale utfall og bør prioriterast høgt.

Verksemder og offentlege etatar kan vurdere fleire tiltak for å gjere tenestene og beredskapen ved tap av ekom meir robust. Det kan vere lurt å opprette ein oppmøteplass i kommunen, der innbyggjarar kan få tilgang til viktig informasjon og eventuelt naudkommunikasjon. Prioritetsabonnement kan bidra til å sikre at kritiske kommunikasjonslinjer blir oppretthaldne ved høg belasting eller så lenge eit av tre mobilnett er oppe. Dual SIM-løysingar kan gi betre dekning og alternativ ved nettverksutfall, slik at ein alltid har tilgang til eit fungerande nettverk.

Med tanke på romvêr bør system for overvaking og varsling vere tilgjengelege og brukarvenlege for relevante aktørar. Sjølv om Nkom ikkje har det direkte ansvaret for desse systema, er det viktig å ha ein tett dialog med dei institusjonane som overvaker og varslar om romvêr. Dette er Meteorologisk institutt, Norsk Romsenter og Universitetet i Tromsø.

For offentlege etatar, statsforvaltarar og kommunar har satellitt-telefonar lenge vore eit viktig beredskapsverktøy for naudkommunikasjon. No satsast det breitt på å ta i bruk geostasjonære satellittar og lågbanesatellittar som transmisjonsberarar for naudkommunikasjon. Dei fleste offentlege etatar, statsforvaltarar, kommunar og naudetatar vil difor bli meir og meir avhengige av satellitt som backup. Det vil difor vere viktig å sjå dette opp mot system for overvaking og varsling.

2.8 SATELLITTBASERTE TENESTER

Riktig opplysning av posisjon og tid er avgjerande for funksjoneringa til ekomnett og ekomtenester, samt infrastruktur og system i andre sektorar[26]. Tids- og posisjonsreferansar blir av bakkebaserte ekomnett henta frå eigne PNT-kjelder (posisjon, navigasjon, tid). Korrekt tid og posisjon kan til dømes bli henta frå satellittbaserte system. Tid kan også hentast frå atomur og distribuerast i ekomnett ved hjelp av NTP[27]-servere for lågpresisjonsbehov og ved hjelp av PTP[28]-løysingar for høgpresisjonsbehov. Ofte blir ein kombinasjon av fleire PNT-kjelder brukt for å sikre redundans.

Frekvensforstyrringar mot radiobaserte PNT-signal kan vere av både tilsikta og utilsikta karakter. Sistnemnde kan vere knytt til utilsikta RF-transmittering, refleksjonar og naturhendingar. Tilsikta hendingar (truslar) mot PNT kan mellom anna omfatte jamming (tenestenektangrep, Denial of Service Attack) og ulike typar spoofing og meaconing (narreangrep, Deception of Service Attacks). Desse kan hindre, degradere eller manipulere informasjon frå PNT-kjelder på veg til mottakar, for å skape ulike typar brot på integritet, konfidensialitet og tilgjenge. Trusselaktørar kan bruke mange ulike fysiske og logiske angrepsflater for å råke PNT, og konsekvensane av slike hendingar kan vere alt frå relativt beskjedne til svært omfattande.

Sidan satellittbaserte navigasjons- og kommunikasjonssystem er spesielt viktige for både opplysning av posisjon og tid, blir dette meir detaljert omtalt:

Satellittbasert navigasjon og kommunikasjon og forstyrringar på desse
Satellittkommunikasjon har historisk sett vore systema som har gitt dekning der andre nett ikkje kan tilby dekning; til havs, i lufta og i avsidesliggjande område.

Satellittbaserte kommunikasjonssystem er sårbare for klassiske cyberangrep som ein finn i tradisjonelle IT-system, ofte retta mot brukar- og kontrollsegment. Det er også mogleg med angrep som fokuserer på satellittar i verdsrommet. Totalberedskapsmeldinga 2025 (side 60) peiker på konsekvensar ved bortfall av satellittbaserte tenester:

«Utfall og forstyrringar av GNSS-signal kan resultere i store økonomiske konsekvensar for samfunnet, eller tap av liv og helse.»

Forstyrringar som hindrar mottak av satellittbaserte navigasjonssystem (ofte kalla Global Navigation Satellite System, GNSS) har auka dei seinare åra. Både tilsikta og utilsikta forstyrringar kan gi mykje av dei same konsekvensane. GNSS-satellittsignal er svake på bakkenivå og er dermed meir utsett for både utilsikta og tilsikta forstyrringar, samanlikna med andre bakkebaserte radiokommunikasjonssystem.

[26] Fleire viktige aktørar er avhengige av ulike tenester som gir nøyaktig posisjon, navigasjon og tid. Døme på dette er telekommunikasjon, søk- og redning, politi, forsvaret og tenester innan finans, kraft og transport.

[27] Network Time Protocol

[28] Precision Time Protocol

GPS-SPOOFING I FINNMARK

Dei austlege delane av Finnmark har i fleire år opplevd GNSS-forstyrringar i luftlag nokre tusen fot over bakken. Desse starta i 2017, og fram til 2022 var forstyrringane sporadiske, nokre dagar her og der. Frå slutten av 2022 og til overgangen 2024/2025 var forstyrringane meir eller mindre konstante, slik at fly som flaug inn og ut av Aust-Finnmark mista GPS. Nkom sine målingar viste at desse forstyrringane var jamming med opphav i russisk territorium på Kola.

I januar 2025 byrja fly i Aust-Finnmark å rapportere om feilaktige GPS-posisjonar i dei områda der dei tidlegare berre hadde mista GPS-dekning. Dei første rapportane melde også om dette problemet på bakkenivå. Målingar og grundigare analysar av pilotrapportar la for dagen at dette var snakk om spoofing, sendt frå Kola. Det viste seg at dei første tilfella av dette eigentleg skjedde i desember 2024, men at det intensiverte seg i januar 2025. Analysane viste også at flya som i utgangspunktet rapporterte om spoofing på bakken eigentleg opplevde etterverknader av den spoofinga dei vart utsette for i lufta, altså at data frå narresignala som mottakarane plukka opp i lufta vart lagra i systemet og dermed «tatt med ned» på bakken.

Spoofing-detektor-verktøy på Internett, basert på opne ADS-B-data, byrja også å plukke opp spoofinga på Kola i januar.

Effekter i cockpiten frå spoofinga var, i tillegg til posisjonsendring til Murmansk-regionen, falske «PULL UP»-kommandoar (tryggingsmekanisme for å unngå kollisjon med terreng); fleire sensorar vart låst i acquisition-modus og heile flysystemet måtte ha ein omstart for å få dei tilbake til normal operasjon; FMSen i flyet vart forvirra av spoofinga og klarte ikkje å filtrere vekk feil (noko den typisk klarer under jamming), noko som resulterte i påverknad på outputen på til dømes fart og høgde frå andre, i utgangspunktet GPS-uavhengige, navigasjonshjelpemiddel; data frå andre sensorar vart presentert ukorrekt; tid i forskjellige system gjekk i utakt.

Nkom sine januarmålingar og informasjon frå flyselskapa indikerte no at forstyrringane ikkje lenger var kontinuerlege og hadde blitt meir sporadiske igjen, og den lågaste høgda som Nkom kunne observere GNSS-forstyrringar frå Russland var 4500 fot over bakken.

Nye Nkom-målingar i mars 2025 kunne ikkje observere spoofing. Om det betyr at spoofinga er heilt vekk eller om den ikkje var aktiv dei dagane målingane føregjekk er uvisst.

Forstyrringane er blitt eit globalt problem ettersom GNSS-system i dag blir brukt overalt i samfunnet. GNSS-mottakarar er ein innvevd teknologi i dagens mobiltelefonar, IoT-einingar, styringssystem for industrien, finans, maritimtrafikk, veg- og lufttrafikk. I tillegg til å bestemme posisjon er GNSS-system også viktige for korrekt opplysning av tid, som er vesenteleg i mange elektroniske system. I 2021 gjekk ein utifrå at det var om lag 6,5 milliardar GNSS-mottakarar i bruk. Fram mot 2031 er det estimert å vekse til 10,6 milliardar GNSS-mottakarar.

Blokkering av GNSS-signal kan påføre store komplikasjonar avhengig av kva det blir brukt til og kor avhengig systemet er av desse signala. Konsekvensen er at GNSS ikkje kan brukast, og tenester som baserer produkta eller funksjonane sine på tilgang til posisjon og/eller tidssynkronisering vil falle heilt vekk eller få redusert yting.

Talet på RFI-hendingar knytt til GNSS som er rapporterte til Nkom dei siste åra har hatt ein kraftig auke. Den same trenden kan ein også sjå i Eurocontrol og andre luftfartsaktørar sine oversikter over GNSS-forstyrringar.

Foto: David Jensen

”

GPS-forstyrrelser i Øst-Finnmark – situasjonsbeskrivelse fra Widerøe

«Siden februar 2022 har GPS-forstyrrelser blitt en del av hverdagen vår i Widerøe når vi flyr i Øst-Finnmark. I starten dreide det seg hovedsakelig om jamming i høyere luftlag. Det skapte riktignok utfordringer for pilotene, men påvirket i liten grad selve flyoperasjonen – fordi forstyrrelsene vanligvis opphørte i det flyene kom i lavere luftlag og startet innflygingen.

I desember 2024 endret bildet seg. Da opplevde vi for første gang spoofing – en mer alvorlig form for GPS-forstyrrelse, hvor systemene om bord blir lurt til å tro at flyet befinner seg et annet sted enn det faktisk gjør. Selv om dette i utgangspunktet er mer alvorlig enn jamming, klarte flyenes systemer å oppdage avviket ved å sammenligne GPS-data med signaler fra konvensjonelt, bakkebasert navigasjonsutstyr. Spoofingen skjedde også i lavere høyder, men heldigvis opphørte problemene stort sett før den kritiske, siste fasen av innflygingen. Likevel er vi bekymret – spesielt fordi slike forstyrrelser kan påvirke systemene som advarer pilotene om fare for terrengkollisjon. At terrenget i Øst-Finnmark er relativt flatt, har hittil gjort det mulig å opprettholde driften med et akseptabelt risikonivå.

Ved inngangen til juni 2025 har situasjonen blitt merkbart verre. Nå ser vi en kombinasjon av både jamming og spoofing, som skjer i enda lavere høyder og dekker større områder. Flere av våre besetninger har rapportert om innflyginger som måtte avbrytes fordi GPS-signalene ble ustabile. Dette har tvunget oss til å bruke konvensjonelle innflygingsprosedyrer basert på bakkebasert navigasjon. Spesielt på kortbaneflyplassene i Øst-Finnmark betyr dette at vi i mindre grad kan gjennomføre landinger under dårlig sikt eller lavt skydekke, sammenlignet med GPS-baserte innflyginger. Vi har hatt tilfeller hvor flyene ikke har fått landet på planlagt destinasjon som følge av jamming, så Widerøe opplever allerede nå at jamming/spoofing har konsekvenser for regularitet.

Hvis dagens situasjon fortsetter – eller skulle bli enda verre – må vi regne med at dette vil påvirke flytrafikken i regionen i større grad. Når høst- og vinterværet setter inn med mer krevende forhold, vil passasjerer i økende grad kunne oppleve at fly ikke kan lande, eller må omdirigeres til andre flyplasser. For oss er sikkerheten alltid det viktigste. Men i praksis må vi under jamming/spoofing-situasjoner operere som vi gjorde for 30 år siden – med mindre presise innflyginger og redusert funksjon for terrengvarslingssystemet. Konsekvensen er en betydelig økt risiko i operasjonen. I verste fall kan det bli nødvendig å innstille større deler av operasjonen i Finnmark, spesielt i situasjoner hvor værforholdene blir utfordrende med tanke på sikt og skydekkehøyde.»

Flight captain/ Safety Advisor Flight Ops Widerøe's Flyveselskap AS

2.8.1 VURDERINGAR OG RISIKOREDUSERANDE TILTAK

Ekomnett og -tenester bør ha tilstrekkeleg redundans med tanke på kvar PNT-informasjon blir henta frå, slik at utfall på eitt system ikkje fører til store utfall eller forstyrringar for heile nettet og/eller tenesta.

Scenario der falsk PNT-informasjon kan skape ringverknader frå den tilbydde tenesta og til brukarar bør analyserast. Vidare bør kjelder til PNT-informasjon isolerast tilstrekkeleg frå kvarandre, både fysisk og implementeringsmessig, slik at ei feilaktig tidsreferanse henta frå ei PNT-kjelde ikkje påverkar bruken av tidsreferansen som er gitt av ei anna PNT-kjelde.

Distribusjon av robust og høgpresis tid er avgjerande for vidare utvikling innan fleire område, til dømes mobilkommunikasjon, kraftsektoren, datasenter og naud- og beredskapskommunikasjon. I nasjonal sikkerheisplan for digital infrastruktur[29] vil regjeringa vurdere å etablere ei nasjonal teneste for distribusjon av nøyaktig tid som tilleggsteneste og redundans til GNSS for å sikre ein motstandskraftig infrastruktur for presis og sporbar tid-/klokkesignal.

Logiske forsvarstiltak bør utvidast til å ikkje berre omfatte tradisjonell forståing av cyberangrep, men også fysiske angrep (slik som tidsspoofing) som kan ha liknande effektar som cyberangrep.

[29] https://www.regjeringen.no/no/dokumenter/nasjonal-sikkerhetsplan-for-digital-infrastruktur/id3117283/

Foto:Gunstein Myhre

3. OPPSUMMERING

Kritisk infrastruktur i Noreg står overfor vedvarande høg risiko, og samfunnet si evne til å fungere heng i stor grad på både fysisk og digital infrastruktur. Svikt i desse infrastrukturane og systema vil medføre alvorlege konsekvensar for leveransen av kritiske varer og tenester som innbyggjarane er avhengige av. EkomROS 2024 peika på cybertrusselen som den mest alvorlege trusselen mot ekom-infrastrukturen med stort skadepotensial, og dette biletet er framleis gjeldande i 2025. Analysen for i år byggjer vidare på den sikkerheitspolitiske situasjonen vi står i.

Den skjerpa sikkerheitspolitiske situasjonen gjer at vi må stille strengare krav til å vere robust og motstandsdyktig i våre digitale infrastrukturar. Både den ferske rapporten frå Riksrevisjonen og den nye nasjonale sikkerheitsplanen peikar på at vi ikkje er på det nivået vi må vere når det gjeld sikkerheit og beredskap. Det er eit stort gap mellom dagens status og det kravde sikkerheitsnivået – eit gap som må lukkast med auka tempo og meir målretta innsats. Nkom kjenner seg igjen i funna og vurderingane i dei to rapportane og ser dei same utfordringane for elektronisk kommunikasjon.

For å sikre forsvarleg sikkerheit og beredskap i dagens trusselbilete må det bli høgare medvit på risiko og etablerast betre risikostyring. Ein må ta omsyn til både tilsikta og utilsikta hendingar – logiske like fullt som fysiske. Tiltak for å gjere sektoren meir motstandsdyktig ber i seg mellom anna meir omfattande risikovurderingar, betre oversikt over utsette tenester og kva som er avhengig av kva, samt ein nasjonal plan for digital infrastruktur. Vi strekar under at beredskap og ei heilskapleg risikostyring krev kontinuerleg overvaking og tilstrekkelege ressursar for å møte utfordringar for ekomsektoren både i dag og i framtida.

Det må vere krav til eit tett og forpliktande samarbeid mellom styresmakter, bransjeaktørar, og både offentlege og private verksemder, for å nå dei nasjonale måla. Ingen aktør kan løfte dette åleine – alle må bidra, både med ressursar, kompetanse og investeringar. Ein felles innsats er nødvendig for å byggje eit digitalt Noreg som er trygt, robust og motstandsdyktig – også i møte med framtidige kriser.

Det noverande trusselbiletet tilseier at det er nødvendig å gå gjennom eksisterande risikovurderingar og tilhøyrande beredskapsplanar – noko Nkom tilrår sterkt at alle verksemder med ansvar for digitale og ekom-relaterte tenester gjer.

4. OPPSUMMERING AV ANBEFALTE TILTAK

Dette kapittelet presenterer ei kortfatta, punktvis liste over tilrådde tiltak innanfor dei ulike områda i kapittelet farer, truslar og sårbarheiter i ekomsektoren (kapittel 2).

Statlege truslar

- Arbeide systematisk med sikkerheitskultur.
- Sikre open kommunikasjon og oppfølging av tilsette.
- Fremje trivsel blant dei tilsette.
- Utføre god leiing.
- Byggje medviten haldning til sikkerheit.
- Samarbeid mellom styresmakter og verksemder for å gi betre effekt i arbeidet med sikring av sjøkablar.
- Raskare behandling av sikkerheits- og tilgangsklareringar.

Verdi – og leverandørkjedar

- Tilbydarar bør ha god oversikt over verdikjeder og leverandørkjeder for å identifisere dei viktigaste faktorane for drift og tenesteproduksjon.
- Ha innsikt i kven ein samarbeider med og er avhengig av, både innanlands og utanlands.
- Datasenteroperatørane må oppfylle krav til forsvarleg sikring og beredskap, med fokus på sikring og varsling.
- Utvikling og bruk av sikre protokollar.
- Etablering av strenge kontrollmekanismar for tilgang.
- Gjennomføring av grundige risikovurderingar

Planlagt arbeid i nettet

- Alt planlagt arbeid må følgje etablerte prosedyrar og sikkerheitskrav for å unngå utilsikta driftsforstyrringar.
- Før ein set i gang arbeid, skal det gjennomførast ei grundig risikovurdering for å identifisere mogelege konsekvensar og nødvendige risikoreduserande tiltak.
- Endringar må testast grundig før implementering, og det bør gjennomførast evalueringar og revisjonar av arbeidet for å lære av eventuelle feil.
- Risiko- og sårbarheitsvurderingar må vere oppdaterte og dekke alle relevante aspekt av arbeidet.
- Det må vere fungerande reserveløysingar for kritiske tenester, slik at ein feil ikkje fører til omfattande tenesteutfall.
- Underleverandørar må jamleg reviderast for å sikre at dei oppfyller krava til sikkerheit, beredskap og kvalitet.
- Det må vere tydelege rutinar for rask og presis varsling til relevante styresmakter og interessentar dersom det oppstår avvik under planlagt arbeid.
- Bruk av styringssystem og system for kvalitetssikring i samband med planlagt arbeid.
- Sidemannskontroll ved endringar som har eit stort konsekvenspotensial.

- Rutinar for tilbakerulling av endringar.
- Test av tilbakerulling.
- Gjennomføring av planlagt arbeid til tider på døgnet der konsekvensen ved feil vil bli mindre.
- Å arbeide for best mogleg systemkunnskap for å forstå korleis konfigurasjons¬endringar kan påverke systemet og korleis feiltilstandar kan oppstå ved konfigurasjon.

Cyberdomenet

- Redusere unødvendig eksponering mot Internett.
- Innføre prinsipp som Zero Trust og Least Privilege for tilgangs- og rettigheitsstyring.
- Ha tilstrekkeleg overvaking av uventa endringar (anomalideteksjon).
- Gjere risikovurderingar av verdi og avhengigheitar for tenesteutsetting av drift, administrasjon og logisk infrastruktur.
- Følgje NSM sine grunnprinsipp for IKT- sikkerheit, samt NIST og CISA sine retningslinjer for IKT-sikkerheit.
- Bruke standardar som ISO27000-serien og IEC 62443 for IT-sikkerheitsstyring og styrking av nettverk.
- Sjå på tiltak gitt av CISA, NSA og FBI for betre grunnsikring og auka deteksjonsevne.

Svindel

- Vere medviten om dei økonomiske og psykologiske konsekvensane av svindel for den fornærma parten.
- Auke bevisstheit om risikoen ved redusert tillit til ekomtenester, som kan føre til meir tidkrevjande alternativ og digital ekskludering.
- Kombinere mobilnummerblokkering med fastnettnummer-blokkering for eit effektivt vern mot misbruk.

Naturhendingar

- Kommunane bør opprette førehandsdefinerte møteplassar for innbyggjarar ved utfall av ekom
- Samfunnskritiske verksemder bør søkje om prioritetsabonnement for mobiltelefonen for personell med beredskapsansvar.
- Alle med beredskapsansvar eller særleg behov bør vurdere «Dual-sim» i mobiltelefonen
- Vurdere å ha ulike abonnement i ulike mobilnett i familien

Satellittbaserte tenester

- Sikre tilstrekkeleg redundans i ekomnett og -tenester for å forhindre store utfall eller forstyrringar ved utfall av eitt PNT-system.
- Isolere PNT-informasjonskjelde frå kvarandre, både fysisk og implementeringsmessig, for å hindre påverking av tidsreferansar.
- Utvide logiske forsvarstiltak til å inkludere både cyberangrep og fysiske angrep, slik som tidsspoofing, som kan ha liknande effektar.
- Vurdere å etablere ei nasjonal teneste for distribusjon av nøyaktig tid som tilleggsteneste og redundans til GNSS.

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