Risikovurdering av ekomsektoren 2021

En sektor i endring

Nasjonal kommunikasjons-myndighet

Foto: Gunstein Myre

Innhold

Hovedside foto: Anders Martinsen

Sammendrag

I årene fremover vil sektoren for elektronisk kommunikasjon gjennomgå store endringer. En viktig driver er 5G, og nye muligheter som denne teknologien bringer med seg for smartsamfunnet, for næringslivet og for industrien.

Nye økosystemer og løsninger innen mobil- og bredbåndstjenester vil prege sektoren. Den digitale grunnmuren vil ha større konvergens mellom faste og trådløse tjenester, internettbaserte tjenester og plattformer, skytjenester og datasenter og spesialiserte/ nisjebaserte kommunikasjonsløsninger. Resultatet er bedre og mer effektive tjenester, men også økt kompleksitet.

For at sektoren kan bidra til effektivisering, innovasjon og næringsutvikling i Norge, må det ligge en grunnleggende tillit i bunnen. Denne tilliten har sektoren i dag, og Norge er et av verdens mest digitaliserte land. Offentlig sektor, næringsliv og industri vil imidlertid vegre seg for å ta i bruk *nye* løsninger, for eksempel basert på 5G, hvis de ikke har tillit til at kvalitet og sikkerhet kan ivaretas.

Nkom ser en risiko i at nye løsninger og økt kompleksitet kan skape uklare ansvarsforhold for sikkerheten. Her er det viktig at både ekommyndigheten, aktørene i ekomsektoren og brukerne - herunder næringslivet og industrien – samhandler proaktivt for å identifisere og håndtere oppdukkende utfordringer.

Tilliten til den digitale grunnmuren vil også utfordres sterkt av utenforstående påkjenninger. I det logiske domenet ventes økt aktivitet innen digitale trusler og angrep. Alvoret understrekes av de alvorlige digitale angrepene på norske kritiske samfunnsfunksjoner siste året.

I det fysiske domenet slår FNs nye klimarapport fast at vi må belage oss på mer ekstremvær i årene som kommer. Nkom ser særlig behov for å styrke regional- og aksessnett. Dette vil kreve økte investeringer i robusthet, redundans og reservestrømforsyning i sektoren.

Om rapporten

- Denne rapporten er en kortfattet beskrivelse av Nkoms årlige risikovurdering av sektoren for elektronisk kommunikasjon (EkomROS). Rapporten skal gi retning for myndigheter, for virksomheter i sektoren, og for virksomheter utenfor sektoren hvor elektronisk kommunikasjon inngår som kritisk innsatsfaktor.

- Nkoms vurderinger er basert på kunnskap og erfaring fra forvaltnings- og tilsynsarbeid i sektoren, og fra EkomCERT. Vurderingene bygger også på trussel- og risikovurderingene fra de norske sikkerhetsmyndighetene (NSM, PST og E-tjenesten).

- Nkoms nettsider har mer informasjon om risikovurderinger for elektronisk kommunikasjon. Her kan kommuner, Statsforvalteren, offentlige og private virksomheter finne veiledning for gjennomføring av egne risikoanalyser for elektronisk kommunikasjon.

Foto: Gunstein Myre

1
Erfaringer fra 2020 og første halvår 2021

Oppsummering

- Det har vært få store utfall i ekomnettene i perioden, men antallet varsler om utfall til Nkom har økt. Fiberbrudd dominerer fortsatt varslingene, og utgjør 50 prosent av alle varsler.
- Omfanget av GPS-forstyrrelser i Troms og Finnmark vedvarer. I perioden har Nkom blitt varslet om 12 hendelser som har påvirket fly- og helikoptertrafikk i fylket.
- Omfanget av telefonsvindel er høyt selv om operatørene klarer å stoppe mye av svindeltrafikken. Nkom er aktiv pådriver i arbeidet med å få redusert omfanget.
- Digitale angrep har økt i volum og blitt mer sofistikerte. Dette treffer alle sektorer, inkludert ekomsektoren. Norske ekom-tilbydere har måttet håndtere løsepengeutpressing med trusler om kraftige tjenestenektangrep.

Foto: Gunstein Myre

En periode med få store utfall i ekomnettene

I 2020 og første halvår 2021 har det vært få hendelser med større utfall i elektroniske kommunikasjonsnett og -tjenester. I hele perioden har det kun vært tre uvær som er definert som ekstremvær av Meteorologisk institutt, to av disse på grunn av høy vannstand. Det tredje var ekstremværet Frank som traff Nord-Norge i januar 2021 og brakte med seg sterk vind. Uværet forårsaket bare mindre og spredte dekningsutfall i mobilnettene.

Målinger av tilgjengelighet og stabilitet i de norske mobilnettene, som gjennomføres årlig av CRNA[1], viser gode resultater også i 2020. Målingene i 2020 var basert på 147 målepunkter spredt rundt i landet tilkoblet Telenor, Telia og ICE sine mobilnett. Tilgjengeligheten i 2020 var over 99,99 prosent på 60 til 80 prosent av de 147 målepunktene, og ytelsen på dataforbindelsene var stabile.

Kvikkleireskredet på Gjerdrum

Kvikkleireskredet på Gjerdrum 30.12.2020 satte i gang en intens og kompleks redningsoperasjon som omfattet både redningstjenestene, private organisasjoner, frivillige organisasjoner og Forsvaret. Nødnett var helt sentralt for koordinering og samhandling, og var operativt hele tiden selv om kapasiteten i perioder ble utfordret.

Mobilnettene til Telenor, Telia og ICE var også oppe under hele hendelsen og sørget for viktig dekning i det berørte området. Mobiloperatørene rapporterte fortløpende driftsstatus til Nkom, og bisto også redningstjenestene med elektroniske spor.

Neste generasjon nød- og beredskapstjenester skal realiseres i de kommersielle mobilnettene. Direktoratet for samfunnssikkerhet og beredskap (DSB) ledet arbeidet med konsept-valgutredning, i samarbeid med Nkom.

[1] «Norske mobilnett i 2020», Tilstandsrapport fra Centre for Resilient Networks and Applications, Simula, 2021.

Fiberbrudd og mobilutfall dominerer varslingene til Nkom

Tilbydere av elektronisk kommunikasjon er pålagt å rapportere til Nkom om uønskede hendelser over en viss alvorlighetsgrad.
De fleste varslene omhandler hendelser som påvirker tilgjengeligheten til tjenestene (utfall).

I 2020 ble Nkom varslet om 160 hendelser.
I løpet av første halvår 2021 har Nkom mottatt varsel om 67 hendelser. Varslingstersklene for utfall er basert på antall mennesker og geografisk område som er berørt, og om tjenestene har betydning for liv og helse. Varslingene til Nkom representerer derfor kun et utvalg av det totale antallet utfallshendelser.

Halvparten av utfallene skyldes fiberbrudd
Dette er tilsvarende som i 2019 og 2018. Fiberbrudd skyldes ofte uhell i forbindelse med grave- og anleggsarbeid og uvær. Fordelingen av andre typer hendelser er også forholdsvis lik som i 2019 og 2018.
Etter fiberbrudd er de innrapporterte feilsituasjonene kategorisert som strømbrudd (16 prosent) frekvensforstyrrelser (12 prosent), programvarefeil (10 prosent), maskinvarefeil (8 prosent) og feil i hjelpeteknisk utstyr (2 prosent).

Halvparten av varslene gjelder utfall på mobiltjenester
Fiberbrudd rammer gjerne både fasttelefoni, fast bredbånd og mobiltelefoni samtidig i et avgrenset geografisk område. En programvarefeil hos en tilbyder kan derimot ramme en spesifikk tjeneste, som for eksempel 4G mobildata, i hele landet.

Utfall i mobiltjenester får erfaringsvis stor påvirkning på folks hverdag og trygghetsfølelse. Av de innrapporterte hendelsene omhandlet omtrent halvparten utfall av mobiltjenester, som mobil tale, mobilt bredbånd og/eller meldingstjenester. Den nest vanligste tjenestekonsekvensen var utfall i faste bredbåndstjenester.

Hendelserfordelt per kategori

- Fiberbrudd (50%)
- Strømbrudd (16%)
- Frevkensforstyrrelser (12%)
- Programvarefeil (10%)
- Hardwarefeil (8%)
- Feil i hjelpeteknisk utstyr (2%)
- Annet (2%)

Foto: Anders Martinsen

Fortsatt mange GPS-forstyrrelser i Troms og Finnmark

I 2017 og 2018 ble det registrert flere hendelser med bortfall eller forstyrrelser av GPS-signaler som påvirket flytrafikken i Øst-Finnmark. Etterretningstjenesten knyttet dette til militær aktivitet på russisk side. Siden da har det hvert år blitt registrert flere tilfeller av GPS-forstyrrelser, særlig i Troms og Finnmark.

I januar 2020 etablerte Nkom, i samarbeid med Avinor og Luftfartstilsynet, en egen varslings-ordning for forstyrrelser av navigasjons-satellittsystemer. Gjennom 2020 og første halvår 2021 har Nkom mottatt 12 varsler om GPS-utfall i fly og helikopter i Troms og Finnmark.

Totalt i hele landet er GPS-forstyrrelser en økende trend, selv om det ble registrert noen færre hendelser i 2020 enn i 2019.

Omfattende telefonsvindel, selv om mye stoppes

Mange opplever å bli oppringt av utenlandske svindlere som påstår å være fra Microsoft. Det pågår kontinuerlig slike svindelhendelser rettet mot norske brukere. Numrene det ringes fra er forfalsket. Dette kalles spoofing.

En annen svindelform er wangiri, som innebærer at svindlere foretar ett ring og kutt fra et høytakstnummer, for å lokke brukeren til å ringe tilbake og bli belastet for anropet.

Tilbydere har gjort flere tiltak som i betydelig grad har redusert omfanget av spoofing og wangiri. Nkom er aktiv pådriver i arbeidet. Samtidig er dette en pågående kamp mot internasjonal kriminalitet der det er ikke mulig å være i forkant av alle svindelforsøk.

En annen betydelig svindeltrend i 2021 er Flubot. Mobilbrukere mottar da SMS, for eksempel forkledd som en melding om postpakke, men med lenke til en app eller en nettside styrt av svindlere. Telenor oppgir at de stopper om lag 20 000 slike svindelmeldinger i døgnet.[2]

[2] «Valgene vi tar - Digital sikkerhet 2021», Telenor, 2021

Økt aktivitet innen digitale angrep

Cyberangrep har det siste året rammet virksomheter i alle sektorer. Av de mest omtalte i Norge er datainnbruddene mot Stortinget høsten 2020 og våren 2021, og løsepengeviruset mot Østre Toten kommune i januar 2021.

I desember 2020 ble det kjent at trusselaktører hadde etablert bakdører i programvaren Orion til den amerikanske programvareleverandøren SolarWinds. Programvaren brukes av ulike virksomheter til å styre nettverk, systemer og IT-infrastruktur. Sårbarheten, som kunne utnyttes til fjernkjøring av kode, ble spredt til over 18 000 virksomhetskunder gjennom programvareoppdateringer. Norske virksomhetskunder var også berørt.

Denne type angrep kalles verdikjedeangrep og kan ramme aktører i alle sektorer. Det siste året er det registrert flere slike angrep, og det forventes flere i tiden som kommer.

Ekomtilbyderne har i 2020 og 2021, som foregående år, håndtert et økende volum av distribuerte tjenestenektangrep (DDoS). Angrepene er rettet både mot tilbyderens kunder og mot tilbyderens egen nettinfrastruktur.

DDoS-utpressing

En tydelig trend det siste året har vært DDoS-angrep kombinert med krav om løsepenger. Virksomheter har da blitt utsatt for et «begrenset» tjenestenektangrep etterfulgt av et utpressingsbrev med trussel om et vesentlig kraftigere angrep, dersom det ikke blir betalt et gitt løsepengekrav i kryptovaluta.

I perioden har flere DDoS-utpressingskampanjer pågått internasjonalt (se faktaboks). Kampanjene har også rammet aktører i Norge. Denne type angrep tilbys og omsettes også som tjenester mellom kriminelle aktører.

EkomCERT har ved flere anledninger gitt råd til norske tilbydere som har blitt rammet. Rådene bygger på erfaringer fra EkomCERTs internasjonale samarbeidsnettverk og har blitt brukt av tilbyderne som underlag for risikovurderinger og for å treffe mer effektive mottiltak.

Nkom EkomCERT

Nkom EkomCERT er den norske ekomsektorens digitale responsmiljø, og utgjør en operativ enhet med kontaktflater nasjonalt og internasjonalt. EkomCERT jobber tett med ekomaktørenes sikkerhetsorganisasjoner, Nasjonalt cybersikkerhetssenter (NSM NCSC) og andre sektorresponsmiljøer (SRM).

EkomCERT har spisskompetanse på det digitale sårbarhets- og trusselbildet generelt, og sektorspesifikke utfordringer spesielt. Ved alvorlige digitale hendelser yter EkomCERT bistand til ekomaktørene i form av informasjons-innhenting, rådgivning og koordinering.

EkomCERT er medlem av de globale sikkerhetsorganisasjonene FIRST og Trusted Introducer.

www.nkom.no/sikkerhet-og-beredskap/nkom-ekomcert

Foto: GreenMountain

2
Trussel- og risikovurdering

Oppsummering

- 5G vil skape helt nye økosystem, og ansvarsforholdene for sikkerhet blir adskillig mer komplekse. En risiko er at kompleksiteten skaper uklare ansvarsforhold mellom tilbydere, leverandører og kunder. Uklare ansvarsforhold kan forsinke innovasjon og utvikling som 5G-teknologien legger til rette for.

- Ekominfrastrukturen konvergerer i økende grad med datasenter- og skytjenesteinfrastrukturen. Datasenter og skytjenester leverer høy grad av sikkerhet til sine kunder. En risiko er likevel at den nasjonale datasenterinfrastrukturen *som helhet* ikke sikres tilstrekkelig for å ivareta samfunnets behov i både fredstid, krise og krig.

- Det ventes økt digitalisering i industri og næringsliv i hele landet, og fortsatt bruk av hjemmekontor. Nkom venter at lokale og regionale ekomtilbydere vil bli en viktigere del av verdikjeden til de nye digitale tjenestene. De mindre ekomtilbyderne kan ha dårligere forutsetninger enn de store til å motstå avanserte trusler og angrep. Dette øker risikoen for at de blir mer attraktive mål for digitale angrep.

- Den norske ekominfrastrukturen vil møte økte påkjenninger fra naturen i årene som kommer. På samme tid vil digitaliseringen av samfunnet stille stadig strengere krav til stabilitet og tilgjengelighet i den digitale grunnmuren. Nkom ser særlig behov for å styrke regional- og aksessnettene. Dersom tilliten til ekominfrastrukturens motstandsdyktighet reduseres, kan det svekke digitaliseringstakten.

Foto: unsplash

Komplekse ansvarsforhold for sikkerhet ved nye 5G-anvendelser

Foreløpig bygger mobiloperatørene ut nye 5G-basestasjoner som gir økt hastighet og kapasitet, mens de fortsatt bruker kjernenett basert på 4G-teknologi. Det fulle potensialet i 5G vil utløses i løpet av de neste par årene når operatørene tar i bruk 5G-teknologien også i kjernenettet. Da legges det til rette for helt nye bruksområder innenfor industri og næringsliv, for massiv IoT og for kritiske kommunikasjonstjenester.

5G-frekvensauksjonen – en viktig milepæl

En viktig milepæl for 5G-utbyggingen ble nådd 30. september 2021. Da avsluttet Nkom auksjonen av viktige 5G-frekvenser i 2,6 og 3,6 GHz-båndene.

Frekvensene ble tildelt Altibox, ICE, Telenor og Telia for en samlet pris på nesten 3,9 milliarder kroner.

Med frekvensene følger det særskilte forpliktelser for utbygging av bredbånd i distriktene, og forpliktelser overfor industri- og nærings-livsaktører slik at de skal kunne ta i bruk 5G til nye industrielle anvendelser.

Med 5G blir mobilnettene en sky-basert arkitektur som legger til rette for dynamiske og skalerbare løsninger tilpasset ulike typer brukerbehov. Mobilnettene kan deles opp i flere virtuelle mobilnett (skivedeling), med dedikerte ressurser og egenskaper for ulik bruk. Tjenester kan produseres på ulike steder, både sentralt og lokalt (edge computing), og driftes med utgangspunkt i ulike typer modeller som private, offentlige eller hybride 5G-nett.

Mange ulike brukerscenarioer og driftsmodeller vil utfordre tilbydere, leverandører, eventuelle tredjepartsaktører, og de som skal anvende tjenestene, i å klargjøre ansvaret for sikkerheten i 5G-tjenesteleveransene. Nkom er også bevisst på at det kan være regulatoriske gråsoner i disse skjæringspunktene.

Dersom viktige ansvarsforhold rundt sikkerhet ikke er tydelige nok, kan det føre til feilsituasjoner og sårbarheter som kan svekke tilliten. I neste omgang kan det legge hindringer i veien for videre innovasjon og utvikling som 5G-teknologien legger til rette for.

Aktuelle tiltak

Nkom vil bidra til å identifisere og håndtere eventuelle regulatoriske utfordringer rundt nye anvendelser av 5G. En arena for å identifisere aktuelle problemstillinger er blant annet 5G Special Interest Group (5G SIG) som Nkom og NSM samarbeider om.

Ekomtilbyderne bør skape bevissthet på ansvarsforhold rundt sikkerhet i utviklingen av nye 5G-tjenester og -anvendelser overfor bedriftskundene. De bør synliggjøre sikkerhetsmessige fordeler og ulemper ved ulike typer brukerscenarioer.

Kommuner og andre offentlige og private virksomheter bør foreta grundige risikovurderinger for å finne egnede modeller tilpasset egen virksomhets behov. De bør sørge for å få synliggjort og avklart ansvaret for sikkerhet mellom egen virksomhet, tilbydere og eventuelle tredjepartsaktører.

Foto: GreenMountain

Behov for helhetlig sikring av den nasjonale datasenterinfrastrukturen

De siste årene har norsk datasenterbransje foretatt betydelige investeringer. Dette er et svært positivt bidrag til målet om å styrke Norges posisjon som datasenternasjon, og dermed legge til rette for at skytjenester kan produseres i Norge.

Datasentre blir i økende grad en integrert del av den elektroniske kommunikasjonsinfrastrukturen – den digitale grunnmuren. I tillegg til at ekomtilbydere leverer konnektivitet til og mellom datasentre, blir også tilbydernes egne tjenester i økende grad produsert som skytjenester i datasentre. Dette gjelder ikke minst for 5G mobiltjenester.

De virksomheter som skal ta i bruk skytjenester, eller som innplasserer eget utstyr i datasentre, har selv ansvaret for å ivareta egen sikkerhet. Skytjenesteleverandørene og datasenteraktørene blir da som «underleverandører» gjenstand for de kravene som kundene setter.

Samtidig er datasenteraktørene per i dag ikke underlagt en helhetlig nasjonal sikkerhets- og beredskapsregulering. Det er derfor en risiko for at den nasjonale datasenterinfrastrukturen som helhet, med de akkumulerte samfunnsverdiene som samles i datasentrene, ikke sikres tilstrekkelig for å ivareta samfunnets behov i både fredstid og i krise og krig.

Regjeringens nye datasenterstrategi[3] åpner for å vurdere en styrket regulering av datasentersikkerheten innenfor rammen av lov om elektronisk kommunikasjon (ekomloven). Nkom mener dette er hensiktsmessig. Nye sikkerhetskrav til datasenter må også balanseres opp mot behovet for konkurranse, næringsutvikling og innovasjon. Dette er viktig for å bidra til at særskilte sikkerhetskrav ikke skaper unødvendige etableringshindre for skytjenester og datasentre i Norge.

NSM peker i sin risikovurdering for 2021[4] på den omfattende utbredelsen av skyteknologi og skytjenester. Skytjenesteleverandører leverer gjerne mer innovative og sikre løsninger enn det enkelte virksomheter selv har kapasitet og kompetanse til.

Spørsmålet er hvordan sikkerheten til tjenestene fungerer i en tilspisset sikkerhetspolitisk situasjon. Store skytjenesteleverandører er ofte lokalisert i utlandet. De baserer seg på digital infrastruktur som krysser mange landegrenser og som er sårbar for sabotasje, ødeleggelse og sikkerhetspolitiske endringer.

[3] «Norske datasenter – berekraftige, digitale kraftsenter», Kommunal- og moderniseringsdepartementet, 2021

[4] «RISIKO 2021 – helhetlig sikring mot sammensatte trusler», Nasjonal sikkerhetsmyndighet, 2021

Aktuelle tiltak

Nkom vil, i henhold til ny datasenterstrategi, bidra til å vurdere en nærmere regulering av datasentersikkerhet i ekomregelverket og annet relevant regelverk.

Ekomtilbyderne må, ved bruk av skytjeneste-/datasenterleverandører i sin leverandørkjede, være bevisst på å ivareta sikkerhet og tilgjengelighet i hele krisespekteret fra fred til krise og krig.

Kommuner og andre offentlige og private virksomheter bør bruke sin bestillermakt til å utfordre og stille krav til sine leverandører av ekomtjenester om hvor/hvordan tjenestene produseres, og hvordan sikkerhet og tilgjengelighet ivaretas også under ekstraordinære situasjoner.

Viktige milepæler for datasenterindustrien i Norge

I 2021 og 2022 settes det i drift fem nye sjøfiberforbindelser mellom Norge og utlandet. Dette er Altibox' «Skagenfiber» (Larvik-Hirtshals), «Englandskabelen» (Stavanger-Newcastle), Bulks «Havfrue» (New Jersey, USA – Kristiansand/Esbjerg) og «Havsil» (Kristiansand-Hanstholm). Tampnet har også utvidet sitt sjøfibernettverk i Nordsjøen med ny forbindelse mellom Egersund og Aberdeen. Disse forbindelsene styrker konnektiviteten mellom Norge og utlandet betydelig.

Foto: Nkom

Foto: Gunstein Myre

Også de mindre tilbyderne kan bli attraktive mål for trusselaktører

Nye teknologier legger til rette for økt digitalisering i industri og næringsliv i hele landet inkludert i distriktene. Etter koronapandemien har også bruken av hjemmekontor økt. Dette innebærer at lokale og regionale ekomtilbydere kan få en viktigere rolle som del av verdikjeden til de nye digitale tjenestene.

Trusselaktører ventes å rette oppmerksomhet mot disse nye digitale tjenestene, og mot svakheter i hjemmekontorløsningene. Nkom forventer dermed at de hundretalls lokale og regionale ekomtilbyderne, som en del av denne verdikjeden, også i større grad vil involveres i angrepskampanjer. Dette kan være angrep rettet mot svakheter i trådløse aksesspunkt, brannmurer og aksessnett. Angrep kan også rettes mot tilbydernes administrative IT-systemer som en inngangsport til driftssystemene.

Mange av de små aktørene har ikke de samme forutsetningene som de store for å bygge opp egne sikkerhetsmiljøer og kompetanse som er dimensjonert for å motstå avanserte digitale angrep. På den annen side blir digital sikkerhet i økende grad en viktig konkurranseparameter. For å opprettholde konkurransekraften i markedet er det viktig at også de mindre aktørene skalerer opp arbeidet med digital sikkerhet.

Kartleggingstilsyn av sikkerhet

Nkom har i 2021 gjennomført et kartleggingstilsyn av sikkerhetsstyringen, herunder digital sikkerhet, hos 20 ekomtilbydere av ulik størrelse og geografisk tilhørighet i forskjellige markedssegmenter.

Tilsynet viser at Nkom bør jobbe videre opp mot særlig de mindre aktørene med tanke på håndtering av det digitale sårbarhets- og trusselbildet.

NSM beskriver situasjonsbildet i 2021 som skjerpet, med et høyere aktivitetsnivå mot norske virksomheter og institusjoner sammenlignet med tidligere år.

PSTs trusselvurdering for 2021[5] peker på at utenlandske etterretningstjenester vil bruke store ressurser på å bryte seg inn i norske datanettverk. Formålet vil først og fremst være informasjonsinnhenting, men PST forventer også operasjoner som har som formål å manipulere informasjon og å sabotere digitale systemer.

Utenlandske etterretningstjenester vil utnytte reduserte digitale sikkerhetsmekanismer bl.a. i hjemmekontorløsninger.

[5] «Nasjonal trusselvurdering 2021», Politiets sikkerhetstjeneste, 2021

Aktuelle tiltak

Nkom styrker arbeidet med digital sikkerhet i sektoren, også med et spesielt søkelys på de mindre bransjeaktørene. Samarbeidet med Nasjonalt cybersikkerhetssenter og de andre sektorresponsmiljøene videreutvikles.

Ekomtilbyderne må vurdere, og håndtere, risikoen for å bli rammet av avanserte digitale angrep rettet mot egen kundeportefølje og som resultat av økt bruk av hjemmekontor. Tilbyderne kan styrke samhandlingen med EkomCERT blant annet gjennom EkomCERTs informasjons- og samhandlingsportal.

Kommuner og andre offentlige og private virksomheter bør følge Nasjonal sikkerhetsmyndighets «Grunnprinsipper for IKT-sikkerhet». De bør være bevisst på at ved bruk av tjenesteutsetting og skytjenester, og bruk av hjemmekontor, så er også bredbånds-/internettleverandøren en sentral del av verdikjeden som må risikovurderes.

Foto: Anders Martinsen

Ekominfrastrukturen utsettes for mer ekstremvær

Den nye klimarapporten til FNs klimapanel som ble publisert i august 2021, slår enda tydeligere fast enn tidligere at menneskeskapte klimaendringer har medført omfattende endringer i atmosfæren, havet og økosystemene.

Ekominfrastrukturen vil utsettes for sterkere påkjenninger i form av ekstremvær og alvorlige naturhendelser i årene fremover. Det kan bli mer ekstrem vind, ekstrem nedbør med påfølgende skred, snø/ising-problematikk og flom i elver og vassdrag. Vi må også forvente langvarige tørkeperioder med påfølgende skog- og utmarksbranner.

Ekombransjen investerte i 2020 til sammen hele 12,6 milliarder kroner i ekomnett og -tjenester, det høyeste investeringsnivået for alle år. Mye av investeringene handler om å gi *tilgang* til ekomtjenester, som gir grunnlag for økt digitalisering og effektivisering av samfunnet.

Gradvis skaper dette en enda sterkere avhengighet til denne infrastrukturen. I tillegg skal kritiske samfunnsfunksjoner, som nød- og beredskapstjenester, realiseres i de kommersielle nettene. Investeringene må derfor i økende grad rettes mot å *forsterke* infrastrukturen.

Nkom ser særlig behov for å forsterke «kanten» av ekomnettene, som regional- og aksessnettene. Dette er den delen av ekominfrastrukturen som er mest sårbar for påkjenninger fra naturen. Det vil kreve økte investeringer i robuste nett, redundans og reservestrømforsyning.

Regionale analyser av samarbeidet med kraftsektoren

I 2019 gjennomførte Nkom en detaljert kartlegging og sårbarhetsanalyse av ekominfra-strukturen i Finnmark. Flere tiltak ble gjennomført gjennom myndighetsfinansiering.

Tilsvarende analyse gjennomføres i Troms i 2021, og Stortingsmelding 28 (2020-2021) – *Vår felles digitale grunnmur*, legger opp til minst fem nye slike regionale analyser.

Nkom har også satt i gang et arbeid sammen med Norges vassdrags- og energidirektorat (NVE) for å styrke det beredskapsmessige samarbeidet med kraftsektoren.

Aktuelle tiltak

Nkom vil følge opp strategien for sikker og robust ekominfrastruktur i Stortingsmelding 28 (2020-2021) – *Vår felles digitale grunnmur*. Nkom jobber i tillegg med å revidere målbildene for ekominfrastrukturen som ble publisert i rapporten «Robuste og sikre nett» (ROBIN) fra 2017.

Ekomtilbyderne må legge vekt på klimatilpasning ved utbygging av infrastruktur. Sikkerhet og robusthet blir i økende grad et konkurransefortrinn. Tilbyderne bør derfor bevisstgjøre, gi veiledning og samarbeide med kunder om sikkerhets- og robusthetsøkende tiltak.

Kommuner og andre offentlige og private virksomheter bør vurdere naturrisiko og sårbarhet i tilknytning til egen kommune/virksomhet og bruke dette ved anskaffelser av kritiske ekomtjenester. De bør vurdere alternative sikkerhetsløsninger- og produkter, og eventuelt uavhengige reserveløsninger. Ved større anskaffelser kan forsterkninger av infrastrukturen være en del av forhandlingen med tilbyder. Det bør følge krav om tilgangsplikt til andre tilbydere for slike forsterkninger for å unngå innlåsningseffekter.
Et annet viktig tiltak for å legge til rette for effektiv utbygging og forsterkning er å registrere infrastruktur og bygge- og anleggsarbeider i Ekomportalen (www.ekomportalen.nkom.no).

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