Nasjonal kommunikasjons-myndighet

EKOMROS 2020:

DEN DIGITALE GRUNNMUREN SATT PÅ PRØVE

Forsidefoto: Gunstein Myre/Nkom

SAMMENDRAG

12. mars 2020 endret trafikkmønsteret på internett seg over natten i Norge, da samfunnet ble stengt ned som følge av koronapandemien. Myndigheter, næringsliv og utdanningssektoren måtte «ekspressdigitalisere», og i mye større grad ta i bruk digitale plattformer og telefon- og videobaserte løsninger – alt over internett.

I det store og hele taklet den underliggende digitale grunnmuren omstillingen. Det var tilstrekkelig kapasitet i transportnettene, fastnettene, mobilnettene og internett, og tilbyderne viste god beredskaps- og omstillingsevne.

Grunnmuren ble satt på en prøve, og besto testen – denne gangen. Samtidig var vi heldige ved at nedstengingen ikke sammenfalt i tid med andre alvorlige hendelser som ekstremvær, flom, strømbrudd, eller større tekniske feilsituasjoner.

Omstillingen etter mars 2020 har vist at det er en grunnleggende tillit til den digitale grunnmuren. Men for å ivareta denne tilliten, kreves kontinuerlig arbeid i ekomsektoren.

Også gjennom 2019 og første halvdel av 2020 ser vi at tilliten stadig utfordres, gjennom alt fra utfallshendelser til telefonsvindel og utpressingsforsøk og avansert digital etterretning.

I år retter Nkom oppmerksomheten mot fire risikoområder, som er ment å komplementere bildet fra tidligere års EkomROS-rapporter. Det ene risikoområdet omhandler skader og brudd på ekominfrastrukturen som følge av naturhendelser. Tilgjengelighet er en fundamental forutsetning for videre digitalisering, og robustheten til infrastrukturen må kontinuerlig styrkes i takt med økte fysiske påkjenninger.

Det andre risikoområdet omhandler de kritiske kjernefunksjonene på internett. Mange sårbarheter og utfordringer knyttet til internett er grenseoverskridende i sin natur, og må håndteres på internasjonalt nivå. Samtidig blir det stadig viktigere å legge til rette for en sikker og grunnleggende funksjonalitet og autonomi i den norske delen av internett.

Det tredje risikoområdet tar for seg den økte betydningen til trådløs kommunikasjon. Det ventes en formidabel vekst i antall enheter som kommuniserer trådløst. Dette vil kreve økt oppmerksomhet på sårbarheter knyttet til dataintegritet og konfidensialitet, samt støy og interferens, jamming og spoofing.

Det siste risikoområdet er knyttet til de komplekse digitale verdi- og leverandørkjedene som ventes med det nye 5G-økosystemet. 5G vil preges av at nye aktører og tredjeparter vil integreres tettere i tjenesteproduksjonen, og hvor vi får sterkt økende bruk av virtualisering, skybaserte løsninger og kompleks automatisering.

INNHOLD

1

INNLEDNING

Virksomheter som tilbyr elektroniske kommunikasjonsnett eller -tjenester (ekom) i det norske markedet skal på bakgrunn av egne risiko- og sårbarhetsanalyser (ROS) ha beredskapsplaner og gjennomføre tiltak for å opprettholde forsvarlig sikkerhet for sine brukere.

Kravet om forsvarlig sikkerhet skal gjelde både i det daglige, i ekstraordinære situasjoner – som vi opplevde under nedstengingen av samfunnet i mars 2020 – og i kriser og krig.

Gjennom den kontinuerlige forvaltingen, tilsynsarbeidet og samarbeidet med aktørene i ekomsektoren, får Nkom god oversikt over nett, tjenester, utviklingsplaner, sårbarheter og risiko. Ekomsektorens digitale responsmiljø, Nkom EkomCERT, henter i tillegg inn og setter sammen informasjon om sårbarheter, trusler og hendelser i det digitale domenet.

Til sammen skaper disse informasjonselementene et viktig fundament for Nkoms egne risikovurderinger.

Nkom er en del av totalforsvaret og har utstrakt sikkerhets- og beredskapssamarbeid med andre sektormyndigheter og regionale myndigheter.

Foto: Gunstein Myre/Nkom

2

ERFARINGER FRA 2019 OG FØRSTE HALVDEL 2020

2019 og første halvdel av 2020 har vært en forholdsvis normal periode med tanke på rapporterte uønskede hendelser til Nkom.

Overordnet opplever Nkom at tilliten til elektroniske kommunikasjonsnett og -tjenester er høy. Norge ligger sammen med de andre nordiske landene (og Nederland) på topp i den europeiske digitaliseringsindeksen DESI [1] .

Den opplevde tilliten og kvaliteten i nettene understøttes av rapporter fra forskningssenteret Simula, som i flere år har gjort målinger av stabilitet og robusthet i de norske mobilnettene [2]. I 2019 var målingene basert på 161 stasjonære målepunkter spredt over store deler av Norge, og 17 målenoder plassert på tog. Den positive trenden de har observert – og særlig etter overgangen fra 2G/3G til 4G – fortsatte også gjennom 2019.

[1] *Digital Economy and Society Index*
[2] *«Norske mobilnett i 2019», Simula, 2020*

2.1 HENDELSER RAPPORTERT TIL NKOM

Tilbyderne er pålagt å varsle Nkom om hendelser som vesentlig kan eller har redusert tilgjengeligheten til ekomnett og -tjenester. Årsakssammenhenger, hendelsenes omfang og alvorlighetsgrad, gir grunnlag for Nkoms videre oppfølging. Oversikten nedenfor baseres på hendelser som er registrert for perioden 1. januar 2019 - 31. juli 2020.

Antall hendelser og hendelseshåndtering

I 2019 mottok Nkom varsler og rapporter på over 100 unike hendelser. I første halvdel av 2020 har antall registrerte hendelser passert 80. Nkom har utarbeidet egne situasjonsrapporter på om lag halvparten av disse, som distribueres til Kommunal- og moderniseringsdepartementet og øvrige nasjonale og regionale beredskapsaktører. Videre har Nkom innhentet utvidede hendelsesrapporter fra tilbyderne for videre gransking og tilsyn, i 14 av disse sakene.

Hendelser fordelt per kategori

KATEGORI	FORKLARING
Fiberbrudd	Utfall som følge av brudd på fiberoptiske kabler på land eller i sjø, for eksempel brudd i forbindelse med gravearbeid eller på grunn av slitasje.
Maskinvarefeil	Utfall som følge av fysiske feil i kritiske komponenter, for eksempel feil i nettverkskort eller fysiske skader eller feilkoblinger i forbindelse med planlagt arbeid.
Programvarefeil	Utfall som følge av logiske feil i kritisk programvare, for eksempel feil i brannmurer, feil i forbindelse med programvareoppdateringer eller endringer i databaser, eller andre former for feilkonfigurering.
Ekstern kraft	Utfall som følge av svikt i ekstern kraftforsyning, for eksempel strøm til basestasjoner.
Intern kraftfeil	Utfall knyttet til interne feil i kraftforsyningen, for eksempel svikt i batteribanker, aggregater eller tavler.
Frekvensforstyrrelser	Frekvensforstyrrelser som rammer trådløs kommunikasjon, f.eks. satellittnavigasjons systemer eller maritim VHF.
Annet	Samlebetegnelse for uønskede hendelser som ikke faller inn under de øvrige kategoriene.

Hendelsene er inndelt i kategorier ut fra feiltype/årsak. Fiberfeil var, som i tidligere år, den hyppigste årsaken til de innrapporterte hendelsene. Dernest kommer utfall av ekstern kraft. Fiberfeil og kraftutfall utgjør 65 % av de innrapporterte hendelsene, noe som er forholdsvis likt som foregående år. Uvær og ekstremvær er ofte underliggende årsak til fiberbrudd og kraftutfall. Graving og anleggsarbeid er også vanlig årsak til fiberbrudd.

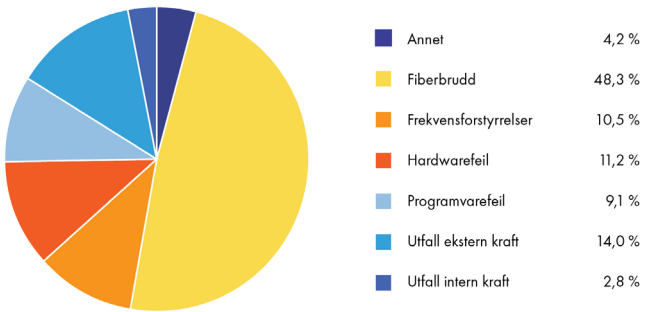
Maskinvare- og programvarefeil var årsak til ca. 20 % av de innrapporterte hendelsene. Andelen av denne type feil har også holdt seg stabil sammenlignet med foregående år.

Antall rapporterte hendelser grunnet kritiske frekvensforstyrrelser øker noe i omfang. Flere av disse gjelder GPS-forstyrrelser i Øst-Finnmark. Dette er et problem som nå har vedvart i noen år, og som påvirker luftfarten i området. Trenden er kortere, men hyppigere tilfeller av slike GPS-forstyrrelser.

Det er etablert varslingsrutiner mellom Nkom, Luftfartstilsynet og Avinor for denne type hendelser. Nkom har også etablert fjernstyrte målestasjoner i området. Øvrige rapporterte kritiske frekvensforstyrrelser gjelder hovedsakelig forstyrrelser på maritim VHF kanal 16 for nødkommunikasjon til sjøs.

Frekvensforstyrrelser som anses mindre kritiske eller ikke medfører umiddelbar fare for liv og helse, inngår ikke i denne statistikken, men håndteres gjennom den ordinære saksgangen.

HENDELSER PER KATEGORI 2019 OG FØRSTE HALVDEL 2020

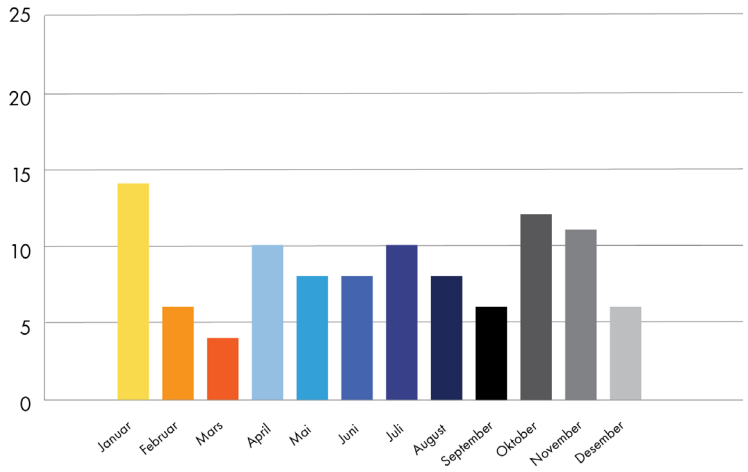


Hendelser fordelt per måned

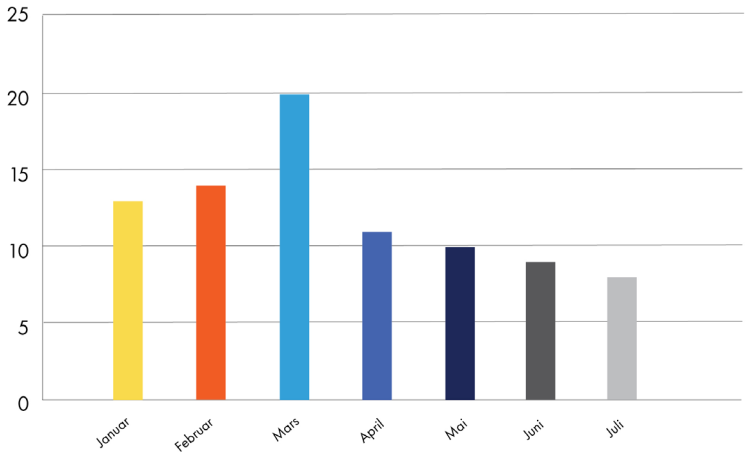
Større utfall relatert til uvær inntreffer i hovedsak om høsten og vinteren. Januar var måneden med flest utfall i 2019. I fjor fikk imidlertid en hendelse i Sogn og Fjordane i månedsskiftet juli-august størst oppmerksomhet. Uvær med påfølgende skred i Jølster medførte bortfall av strøm og ekomtjenester, og forhindret redningspersonell som arbeidet i skredområdet.

I første halvdel av 2020 ble det rapportert flest hendelser i mars, mens antallet gikk suksessivt ned fra april til og med juli.

HENDELSER FORDELT PER MÅNED 2019



HENDELSER FORDELT PER MÅNED FØRSTE HALVDEL 2020

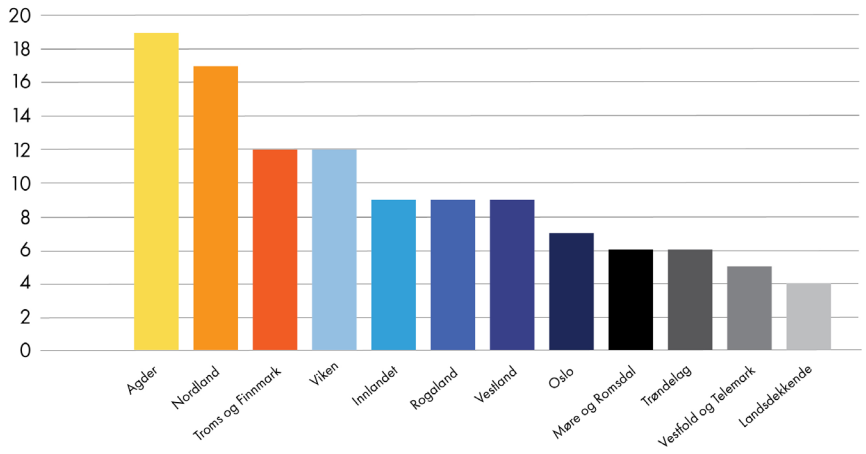


Hendelser fordelt per fylke

Fylkene med flest rapporterte hendelser i tidsperioden er Agder i sør og Nordland, Troms og Finnmark i nord. Til sammen utgjør hendelser i disse tre fylkene om lag 40 prosent av det totale rapporterte antallet.

Nkom er kjent med sårbarhetene i ekominfrastrukturen i disse fylkene. Derfor er områdene også prioritert gjennom «Forsterket ekom»-programmet, hvor Nkom bidrar med tilskudd for å styrke reservestrøm og transmisjon på strategisk utvalgte basestasjoner. I tillegg har Nkom gjennom «Finnmarksprosjektet» kartlagt ekominfrastrukturen i Finnmark og vurderer nå sårbarhetsreduserende tiltak i dialog med aktørene i området.

HENDELSER PER FYLKE 2019 OG FØRSTE HALVDEL 2020



FEILRUTING 113

19. februar 2019 førte en feil hos en operatør til at deres abonnenter i et spesifikt geografisk område ikke hadde tilgang til nødnummeret 113. Feilen oppsto på grunn av en svikt i underliggende informasjonssystemer. Det gikk i overkant av fem timer før feilen ble oppdaget til den ble løst.

Nkom har fulgt opp hendelsen i etterkant, og vedtatt overtredelsesgebyr i saken.

STENGING AV ALTA FLYPLASS

Under en politiaksjon i Alta 29. februar 2019 påla politiet nedstenging av mobilnettene i området rundt Alta flyplass. I nødstilfeller kan politiet kreve slik nedstenging, for eksempel for å hindre at mobilnettet kan brukes til fjernutløsning av bomber. Grunnet beliggenheten til flyplassen ble Alta sentrum og nærliggende områder også berørt av nedstengingen. Dekningen var borte i underkant av to timer.

Det er utarbeidet operative prosedyrer for Nkom, politiet og tilbyderne for å håndtere slike hendelser.

FEIL PÅ BANKID

Torsdag 20. juni 2019 opplevde BankID-systemene stor ustabilitet og utilgjengelighet store deler av dagen. Feilen ble utløst av uvanlig høy trafikk som rammet de underliggende systemene. Dette rammet både BankID med kodebrikke og BankID på mobil. Det ble gjort flere tiltak for å prøve å stabilisere situasjonen, før feilen ble løst senere på kvelden.

Elektronisk signatur som BankID er underlagt lov om elektroniske tillitstjenester. EU-forordningen eIDAS legger til rette for bruk av slike tjenester på tvers av EU og EØS. Nkom fører tilsyn med at de norske tilbyderne av slike tillitstjenester oppfyller forordningens krav.

EKSTREMVÆR UTLØSTE SKRED I JØLSTER

Store mengder nedbør utløste i månedsskiftet juli-august i 2019 flere skred i Jølster i Sogn og Fjordane. Dette førte til bortfall av både mobil- og fastnett, og strøm. Bortfallet vanskeliggjorde situasjonen for de som var innesperret av raset, for redningspersonellet og for de pårørende.

Etter hendelsen har Nkom, på oppdrag fra Kommunal- og moderniseringsdepartementet kartlagt eksisterende og kommende teknologi for transportable basestasjoner som potensielt kan bidra til å raskere gjenopprette midlertidig mobildekning ved slike hendelser [3].

UTFALL PÅ INTERNETTRAFIKK MOT UTLANDET

Søndag 30. august 2020 oppsto det internasjonalt store internettproblemer som følge av en konfigurasjonsfeil på trafikkrutingen hos en av verdens største teleoperatører. Feilen berørte også norske internettilbydere som var tilknyttet denne operatøren for å rute trafikk mot utlandet. En norsk tilbyder opplevde ustabilitet og bortfall av internettrafikken i overkant av fem timer som følge av dette. Internettjenester blir i stadig økende grad en integrert del av både dagliglivet og kritiske samfunnsfunksjoner.

Hendelsen er illustrerende for hvordan en «liten feil» i en kompleks transnasjonal digital verdikjede kan forplante seg, og også alvorlig påvirke tilgang til tjenester i Norge.

---

[3] *«Etablering av midlertidig mobildekning ved utfall», Nkom 2019*

Foto: Anders Martinsen/Nkom

Hendelser rapportert til ENISA

Europeiske ekommyndigheter rapporterer årlig om større uønskede hendelser til EUs sikkerhetsorgan ENISA [4]. På bakgrunn av dette publiserer ENISA årlig en rapport over funn og større trender innen elektronisk kommunikasjon på et overordnet europeisk nivå.

I rapporten [5] for 2019 har det blitt rapportert ca. 160 hendelser, noe som samsvarer med antallet fra tidligere år. Den vanligste årsaken til uønskede hendelser er programvare- og maskinvarefeil. Disse utgjør i overkant av halvparten av alle innrapporterte hendelser.

Litt over en tredjedel av hendelsene er forårsaket av en tredjepart, det vil si underleverandører, entreprenører og andre leverandører som tilbyderne er avhengige av. Hendelser forårsaket av tredjepart er kategorien som har økt mest.

Naturhendelser og hendelser forårsaket av menneskelige feil har også økt siden forrige rapport.

Tilsiktede hendelser, som cyberangrep og fysisk sabotasje/skade, utgjør ca. fem prosent av innrapporterte hendelser.

Over 50 prosent av hendelsene berørte mobiltelefoni, både data- og taletrafikk. Bredbånd og fasttelefoni utgjorde rundt 30 prosent av rapportene, men ofte var flere tjenester berørt samtidig ved feil.

2.2 NUMMERBASERT SVINDELAKTIVITET

Mange har opplevd å bli oppringt av utenlandske svindlere som påstår å være fra Microsoft. Det pågår kontinuerlig slike svindelhendelser rettet mot norske brukere. Daglig sperrer tilbyderne tusenvis av anrop fra eller til utlandet, men mange anrop slipper dessverre gjennom.

Prinsippene for internasjonal ruting av telefonitrafikk er bygget på tillit mellom aktørene i verdikjeden, og svindelmetodene utnytter denne iboende tilliten. Anrop rutes gjerne via flere nett i retning Norge, med det formål at tilbakesporing skal være vanskelig.

Nkom jobber aktivt med bransjen for å forsøke å begrense omfanget av ulegitimert adressemanipulering. Nasjonalt leder Nkom ekspertgruppen «Arbeidsgruppe Nummer», som har nedsatt en egen undergruppe som jobber med aktuelle mottiltak.

Tidligere er det etablert en nasjonal bransjenorm om nummervisning [6].

Internasjonalt er det flere telekommunikasjonsorganisasjoner, som ITU, CEPT og GSMA, som jobber med disse problemstillingene. Blant annet deltar Nkom i en arbeidsgruppe under CEPT, som jobber med tiltak for å redusere spoofing og øke tilliten til adresser i elektronisk kommunikasjon.

I 2019 la Nkom til rette for en dialog mellom en tilbyder og Kripos for å forbedre prosessene for å anmelde og stoppe utbetalinger til kriminelle etter PABX-svindel. Det er avgjørende at politiet raskt gir tilbyderne slike anmeldelsesbekreftelser, som tilbyderne igjen kan henvise til sine internasjonale partnere for å stoppe utbetalinger.

Nkom har i 2020 også vært i dialog med amerikanske myndigheter om deres tiltak på området. Blant annet vil de fra 2021 innføre en autentiseringsløsning kalt STIR/SHAKEN, som innebærer autentisering av telefonanrop mellom amerikanske tilbydere ved hjelp av digitale sertifikater.

---

[4] *European Union Agency for Cybersecurity*
[5] *«Telecom Services Security Incidents 2019 – Annual Analysis Report», ENISA, 2020*
[6] *Se: https://www.nkom.no/telefoni-og-telefonnummer/telefonsvindel*

NUMMER-SPOOFING

Nummer-spoofing vil si å urettmessig manipulere det nummeret det ringes fra (A-nummeret), og som vises på mottakers telefon. Hensikten med spoofing er at anropet skal fremstå som å være et vanlig anrop. I virkeligheten kan det være internasjonale svindlere som ved å utgi seg for å være for eksempel fra Microsoft, vil forsøke å lede brukeren frem til å oppgi kortinformasjon.

Februar 2020 var en aktiv spoofing-måned.
Telia estimerer å ha sperret over 250 000 samtaler denne måneden.

WANGIRI

Wangiri er japansk og betyr «ett (ring) og kutt». Svindlerne ringer via høytakstnummerserier til et stort omfang norske brukere. Etter ett ring legges det på. Svindelen skjer ved at mottaker ringer tilbake og blir belastet for anrop til høytakstserien.

Den første uken i november 2019 blokkerte Telia over sju millioner slike anrop fra å treffe sluttbrukere i Norden. Om lag 20 % av disse var rettet mot norske brukere.

PABX-SVINDEL

PABX-svindel skjer ved at aktører hacker en bedrifts telefonsentral og så begynner å ringe opp et stort antall utenlandske høytakstnummer kontrollert av svindleren. Hvis et angrep f.eks. pågår uoppdaget over en helg, kan det ha påløpt store summer.
Tilsvarende kan skje ved å misbruke et større antall SIM-kort.

PABX-svindel har et mindre omfang, men innebærer større beløp per svindel. En tilbyder estimerte å ha over 20 slike saker i 2018. Enkelte saker kan omfatte beløp i hundretusenkroners-klassen.

2.3 DET DIGITALE ROM SETT FRA EKOMCERT

Nkom EkomCERT er ekomsektorens digitale responsmiljø i Norge. EkomCERT jobber tett med ekomsektorens sikkerhetsorganisasjoner, Nasjonalt cybersikkerhetssenter (NCSC) og de andre sektor-responsmiljøene (SRM) i Norge. Responsmiljøet varsler og yter bistand til tilbydere og andre aktører i sektoren med utgangspunkt i avanserte analyseverktøy og spisskompetanse på sektorspesifikke trusler og sårbarheter i det digitale domenet.

Utnyttelse av sårbarheter i nettverksutstyr

I perioden 2019 og første halvår 2020 har det vært en jevn strøm av nyoppdagede sårbarheter knyttet til maskinvare eller programvare på nettverksutstyr, eller i nettverksprotokoller.

I 2020 har det vært flere eksempler hvor det har gått kort tid fra kritiske sårbarheter har blitt publisert til de har blitt aktivt utnyttet. For eksempel publiserte F5, en produsent av avansert nettverksutstyr, en kritisk sårbarhet den 1. juli 2020, som gjorde det mulig å få urettmessig administratortilgang til systemet.

Sårbarheten gjaldt anslagsvis 14 000 systemer på verdensbasis, inkludert i Norge, og den 4. juli ble det rapportert om aktiv utnyttelse. Det gjensto da fortsatt 8 500 systemer som ikke hadde lukket sårbarheten.

Det totale antallet sårbarheter som publiseres har økt jevnt de siste årene. EkomCERT ser at dette medfører et stadig økende press og kompetansekrav på aktørene i sektoren. Arbeidet med å identifisere og analysere stadig flere sårbarheter, og kunne prioritere de riktige sårbarhetsreduserende tiltakene for egen virksomhet, er krevende.

EkomCERT monitorerer og analyserer sårbarheter i nettverksutstyr, og varsler videre om sårbarheter som kan ha særlig relevans for aktørene i ekomsektoren.

Utfordringer knyttet til DNS

DNS [7] er en kritisk funksjon på internett for å knytte domenenavn sammen med IP-adresser. En ofte utnyttet svakhet i DNS gjør at angripere kan injisere falske svar på domenenavnoppslag som så ruter trafikken til falske nettsteder hvor de kan tilrane seg for eksempel brukernavn, passord og kortopplysninger.

Økt bruk av sikkerhetsutvidelsen DNSSEC [8], som hindrer muligheten for å injisere falske svar i domenenavnoppslag, har på den ene siden bidratt til å redusere dette problemet. Imidlertid ser det ut til at trusselaktørene nå flytter fokus til å utnytte sårbarheter i administrative tilganger hos forhandlere av domenenavn (registrarer).

Ved å tilegne seg slike urettmessige tilganger kan de endre selve oppføringene av DNS-servere, og dermed plassere seg som et mellomledd for å hente ut informasjon.

En annen endring som EkomCERT følger med på er det økte omfanget av DNS over HTTPS (DoH). Her sendes ikke domenenavnforespørselen til internettleverandørens DNS-servere. I stedet sendes forespørselen som vanlig kryptert webtrafikk til DNS-servere kontrollert av innholdsprodusenter, som for eksempel Google.

DoH er i dag gjerne standardinnstillinger i operativsystem, telefoner og nettlesere som kommer fra disse produsentene. DoH sikrer at DNS-trafikken krypteres gjennom nettene, men samtidig flyttes DNS-oppslagene gjerne til servere utenfor landets grenser. Dette svekker den nasjonale kontrollen med DNS.

For internettleverandørene reduseres effekten av å bruke DNS for eksempel til å tilby foreldrefiltre, eller til å sikre lovpålagte filtreringer av nettsider som inneholder overgrepsmateriale av barn.

Tiltak mot BGP-kapring

Border Gateway Protocol (BGP) er en rutingprotokoll som benyttes for å binde sammen nettene som utgjør internett. BGP lar de ulike nettverksoperatørene annonsere hvilke adressesegmenter som benyttes i deres nett, og lære korteste vei til andres nett og adresser.

BGP-kapring innebærer at en operatør annonserer adressesegment de ikke rettmessig opererer, slik at internettrafikken rutes til eller via nett den i utgangspunktet ikke skal gå. Motivasjonen for å utføre BGP-kapring kan være å utføre tjenestenektangrep, avlytte trafikk eller introdusere forfalskede tjenester. Men feilruting kan også skje utilsiktet, for eksempel på grunn av konfigurasjonsfeil.

En av de større hendelsene i 2020 skjedde 1. april, da en russisk internettilbyder feilaktig annonserte 8 000 adresseblokker de selv ikke eide eller kontrollerte. Disse blokkene inkluderte internettadressene til store leverandører av skytjenester, blant annet Google, Facebook og Amazon. Trafikk som var ment for disse skytjenesteleverandørene ble da feilaktig rutet og forkastet.

Svakheter i BGP er i sin natur en global utfordring som ikke alene kan løses innenfor en nasjonal kontekst. I Norge bidrar EkomCERT inn i forskningsprosjektet GAIA, ledet

---

[7] *Domain Name System*
[8] *DNS Security Extension*
[9] *Distributed Denial of Service Attack*

av Simula, som ser på sårbarheter og mottiltak knyttet til kompleks og grenseoverskridende digital infrastruktur og tjenesteproduksjon. Her inngår blant annet forskning på metoder for monitorering og varsling av BGP-kapring.

Utpressing ved bruk av tjenestenektangrep

Distribuerte tjenestenektangrep (DDoS [9]) er dagligdagse hendelser i norske ekomnett. Angrepene er som oftest rettet mot, og rammer, spesifikke sluttkunder eller sluttkunders tjenester. I noen tilfeller blir trafikkbelastningen så stor at den kan påvirke flere kunder, eller i verste fall ramme stabiliteten og tjenesteproduksjonen til hele nettet. Tilbyderne gjør kontinuerlig tiltak for å redusere effektene av slike DDoS-angrep i egne nett og mot sine kunder.

Internasjonalt har det vært en markant og vedvarende økning i antall DDoS-angrep etter at koronapandemien inntraff. Dette synes å være motivert av den økte effekten av slike angrep når bruken av digitale internettbaserte løsninger har økt. Blant annet har sikkerhetsselskapet Kaspersky rapportert at antall DDoS-angrep rettet mot utdanningssektoren og e-læring økte med to til fem ganger i første og andre kvartal av 2020, sammenlignet med 2019. Den generelt økte trafikken legger også beslag på mer av den tilgjengelige båndbredden, slik at skadevirkningene av DDoS-angrepene potensielt blir større.

I 2020 har det også vært rapportert om en internasjonal "ransom-DDoS"-kampanje, som også har truffet Norge. Angrepet innebærer at kriminelle sender løsepengekrav til en bedrift eller organisasjon med trussel om kraftig DDoS-angrep dersom løsepenger ikke utbetales. Kampanjen har blant annet rettet seg mot underliggende infrastruktur som DNS. Flere europeiske internettilbydere har rapportert om driftsforstyrrelser som kan knyttes til dette. EkomCERT har hatt en aktiv rolle i analyse og varsling av kampanjen.

Datalekkasjer

Det ble i 2019 omtalt flere kampanjer hvor avanserte trusselaktører utførte målrettede angrep mot ekomtilbydere. En kampanje, omtalt som "Operation SoftCell", involverte kompromittering av 12 ulike ekomtilbydere i Afrika, Europa, Midtøsten og Asia.

Undersøkelser fra sikkerhetsselskapet Cybereason antyder at kampanjen har pågått siden 2012, og at angriperne hadde hatt langvarige tilganger til administrative funksjoner hos de ulike tilbyderne. Videre benyttet de etter hvert systemtilganger til å hente ut kunders telefonlogger og lokasjonsdata. Den operasjonelle kontrollen var så omfattende at den også potensielt kunne ha blitt benyttet til både avlytting og sabotasje av drift. Kampanjen viser dermed at trusselaktørene ikke bare har vilje, men også tilstrekkelig evne og ressurser.

Løsepengevirus er en annen trend på fremmarsj, som også rammer ekomtilbydere. For eksempel ble Telecom Argentina offer for løsepengevirus 18. juli 2020. Siden 2019 er det også blitt mer vanlig at innhold på datamaskiner ikke bare krypteres men også hentes ut, med trussel om at de blir lekket på internett. For selskaper omfattet av den europeiske personvernforordningen GDPR med høye bøterammer, kan trusselen om eksponering av kunders personlige data være et ekstra pressmiddel for trusselaktørene.

Lekkede data er handelsvare, blant annet på det mørke nettet. EkomCERT har verktøy og kompetanse som bidrar til å identifisere og varsle om handel av stjålne data knyttet til norske ekomtilbydere.

2.4 SEKTORENS HÅNDTERING AV KORONAPANDEMIEN

12. mars 2020 innførte regjeringen de mest inngripende tiltak Norge har innført i fredstid, for å hindre spredning av covid-19. Tilbyderne ble pålagt å rapportere til Nkom daglig om driftssituasjon og utfordringer, og det ble etablert en tett beredskapsdialog mellom Kommunal- og moderniseringsdepartementet, Nkom og tilbyderne for å fortløpende løse de praktiske utfordringene som oppsto innad i sektoren.

Foto: Gunstein Myre/Nkom

Tilbyderne rapporterte om en markant økning i trafikken de første dagene etter nedstengingen, men kapasiteten i nettene var i hovedsak tilstrekkelig til å håndtere situasjonen. Etter nødvendige tekniske tilpasninger de første dagene etter nedstengingen, var tilbyderne i stand til å opprettholde en sikker og stabil driftssituasjon.

I praksis opplevde mange likevel kapasitetsproblemer på internett den første tiden etter nedstengingen. Disse problemene var imidlertid knyttet til selve internett-applikasjonene, og ikke til kapasiteten på nettverkslaget på internett. Den plutselige økningen i bruk av hjemmekontor og hjemmeskole førte blant annet til at bedriftenes VPN-forbindelser og videokonferanseløsninger, og skolenes læringsplattformer ble overbelastet. Disse løsningene ble da etter hvert oppskalert.

Situasjonen for elektronisk kommunikasjon i Norge speilet også situasjonen ellers i Europa. Sammenslutningen av europeiske tilsynsmyndigheter for elektronisk kommunikasjon, BEREC [10] , gjennomførte fra mars 2020 en informasjonsinnsamling om trafikkhåndteringen i de ulike landene.

Nedstengingene medførte en generell trafikkøkning på mobile og faste nett i de europeiske landene, men ingen rapporterte om større kapasitetsutfordringer.

Under koronapandemien ble det også rapportert om høyt antall korona-relaterte registreringer av domenenavn, og det ble gjort tiltak for å motvirke eventuell misbruk av DNS [11] til svindel eller lignende. Nærmere undersøkelser har imidlertid vist at antallet av ondsinnede registrereringer blant disse har vært relativt lavt.

I følge den europeiske sammenslutningen av registerenheter for landkodedomener CENTR [12] , har pandemien ikke har hatt signifikant innvirkning på DNS med hensyn til registreringer av domener eller nivå av misbruk.

[10] *Body of European Regulators for Electronic Communications*
[11] *Domain Name System*
[12] *Council of European National Top-Level Domain Registries*

Foto: Anders Martinsen/Nkom

3

SAMFUNNSMESSIGE OG TEKNOLOGISKE UTVIKLINGSTREKK

3.1 ELEKTRONISK KOMMUNIKASJON UTGJØR EN SENTRAL BRIKKE I TRUSSELBILDET

De årlige trussel- og risikovurderingene fra Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) er viktige kilder i Nkoms sikkerhetsarbeid. Nkom leder også Ekomsikkerhetsforum, som samler sikkerhetsmyndighetene og tilbyderne underlagt sikkerhetsloven, til gjensidig trusselinformasjonsutveksling på gradert nivå.

Det overordnede trussel- og risikobildet viser at elektronisk kommunikasjon i stadig økende grad inngår som et sentralt virkemiddel for etterretnings- og trusselaktivitet i og mot Norge. Videre utgjør den digitale grunnmuren også et mål i seg selv for trusselaktørene.

NSM: Sammensatt virkemiddelbruk

NSM fremhever i sin risikorapport [13] tre risikofaktorer for nasjonal sikkerhet:

- *Samfunnets økende avhengighet av elektronisk kommunikasjon og satellittbaserte tjenester og den fundamentale avhengigheten av kraft.*
- *Økende avhengighet av digitale infrastrukturer og verdikjeder som strekker seg utover våre grenser.*
- *Sammensatt virkemiddelbruk i form av blant annet strategiske oppkjøp, investeringer og påvirkning.*

Etterretningstrusselen mot Norge beskrives som omfattende og med bredt nedslagsfelt. Etterretningstjenester bistår eget næringsliv med omfattende industrispionasje, og mange land bruker store ressurser og avanserte metoder for å skaffe informasjon eller fortrinn for å ivareta sine nasjonale interesser. Blant virkemidlene er nettverksoperasjoner, fysisk og digital kartlegging, påvirkningsoperasjoner, rekruttering av personer, strategiske investeringer, og avlytting av rom og telefontrafikk.

PST: Digital kartlegging og sabotasje

PST vurderer [14] følgende trusler som de mest alvorlige:

- *Spionasje mot regjeringen, Stortinget og Forsvaret.*
- *Digital kartlegging og sabotasje av kritisk infrastruktur.*
- *Terrorangrep utført av enkeltpersoner motivert av høyreekstrem eller ekstrem islamistisk ideologi.*

I følge PST foregår stadig mer av trusselaktiviteten rettet mot grunnleggende nasjonale interesser i det digitale rom. Et digitalisert samfunn og dets avhengighet av ekom medfører økt sårbarhet og gir muligheter for spionasje, manipulasjon og sabotasje. Datanettverksoperasjoner kan påføre staten og samfunnet stor skade, både økonomisk, sikkerhetsmessig og politisk.

Fremmede staters etterretningstjenester vil det kommende året samle inn sensitiv informasjon om alt fra strategier og satsningsområder til produktutvikling og teknologisk innovasjon. Virksomheter innen elektronisk kommunikasjon er blant de virksomheter som anses som særlig utsatte mål.

[13] "Risiko 2020", NSM, 2020
[14] "Nasjonal trusselvurdering 2020", PST, 2020

Spionasje vil rette seg mot underleverandører så vel som hovedleverandører av tjenester og produkter. Mindre virksomheter kan være særlig utsatte, ettersom disse i mindre grad har avsatt tilstrekkelig ressurser til eget sikkerhetsarbeid.

I tillegg viser PST til at utenlandske tjenester også i 2020 vil samle inn kontaktinformasjon til ansatte i norske virksomheter. Telefonnumre og e-poster vil danne utgangspunkt for målrettet teknisk innhenting gjennom for eksempel avlytting og nettverksinfiltrasjon.

E-tjenesten: Økt utnyttelse av teknologiske ikke-militære virkemidler

E-tjenesten viser [15] til at den teknologiske utviklingen har medført at ikke-militære virkemidler i økende grad kan brukes som alternativ til militær makt. Dette kan være økonomisk maktmisbruk, desinformasjonskampanjer, overvåkingsaktivitet og nettverksoperasjoner.

Faktorene som preger trusselbildet for Norge og norske interesser er nært knyttet til Russland og Kina. Spesielt vises det til Russlands gradvise styrking av forsvaret i nordområdene med en rekke nye kapabiliteter. Øvingsaktiviteten i 2019 viser at Russland har kommet langt i å bygge en dynamisk militærmakt med evne til å tilpasse virkemiddelbruk til den enhver tid rådende situasjon.

Både Russland og Kina har interesse av å utfordre den USA-dominerte verdensorden. «Den nye Silkeveien» er en av Kinas strategier for å få til dette. I følge E-tjenesten legger dette grunnlag for en storstilt, global etterretningskapasitet, der kontroll over 5G-nettverk, fiberkabler og smartby-systemer gir mulighet til å samle inn enorme datamengder. E-tjenesten anser Norge for å være blant målene i Silkeveistrategien, og Kinas interesse for Arktis er økende.

[15] *"Fokus 2020", E-tjenesten, 2020*

3.2 DIGITAL TILLIT – EN FORUTSETNING FOR FUNGERENDE EKOM

Tillit er en fundamental forutsetning for å oppnå god effekt av digitaliseringen i samfunnet. Myndigheter, næringsliv og privatpersoner vil vegre seg for å gjennomføre elektroniske transaksjoner om de ikke har tillit til sikkerheten på internett og i de underliggende systemene. Pasienter må kunne stole på at medisinen de får utlevert via e-resept på apoteket samsvaret med det legen har skrevet ut. Denne tilliten underbygges av en sikker digital grunnmur.

Fra underforstått tillit til verifisert tillit

Inntil 80-90-tallet var de europeiske teletilbyderne stort sett nasjonale monopolister og del av den offentlige forvaltningen. Verdikjedene var oversiktlige og samhandling mellom nettene var bygget på en *underforstått* og gjensidig tillit. På samme måte vokste internett ut av forsknings- og universitetsmiljøer der tilliten mellom de sammenkoblede nettene i starten var underforstått.

I dag kan ikke slik tillit legges til grunn, og kommunikasjonssystemene må i større og større grad *verifisere* hverandres identitet før tillit kan etableres og data utveksles trygt. Tilbyderne jobber derfor med å bygge inn mekanismer for å kunne kontrollere og verifisere både integritet og autentisitet i disse systemene og protokollene. Ved å utvide de gamle protokollene med ny sikkerhetsfunksjonalitet, «ettermonteres» i praksis sikkerheten.

Likevel er man bundet av de tidligere designvalgene, og selve systemene er derfor ikke utviklet med hensyn til «security by design». Selv om protokollene med dette blir sikrere, øker også kompleksiteten, og verdikjedene blir mer omfattende. Videre øker også antall aktører som inngår i verdikjedene.

Tillitstjenester

Elektronisk identifikasjon (eID) og tillitstjenester har til hensikt å sikre validitet og tillit elektronisk. De er en viktig forutsetning for å

bruke digitale tjenester på en sikker måte. Lov om elektroniske tillitstjenester har som formål å gi et felles grunnlag for elektronisk samspill mellom bedrifter, borgere og offentlige myndigheter på tvers av landegrensene i EU/EØS.

Kvalifiserte tilbydere av tillitstjenester er underlagt tilsyn av Nkom, og er pliktig til å rapportere sikkerhetshendelser. Denne informasjonen brukes blant annet til å kartlegge potensielle sårbarheter, og bygge opp under tilliten til disse tjenestene.

Kommunikasjonskontroll versus kommunikasjonsvernet

Tilbyderne har etter ekomloven plikt til å legge til rette for politiets lovbestemte tilgang til informasjon og kommunikasjon. Dette inkluderer blant annet kommunikasjonskontroll – avlytting og sporing av mistenktes kommunikasjon. I praksis innebærer dette å legge til rette for politiets tilgang til sentrale punkter i tilbyderens nett.

Tilrettelegging for kommunikasjonskontroll må balanseres mot tilbydernes plikt til å ivareta den enkelte brukers kommunikasjonsvern. Den teknologiske utviklingen har imidlertid gjort at det å legge til rette for effektiv *kommunikasjonskontroll* og samtidig sikre *kommunikasjonsvernet* har blitt mer komplisert.

Dette dilemmaet ser vi blant annet ved kommunikasjonskontroll av utenlandske mobilabonnenter som gjester i norske 4G-mobilnett. Selv om en utenlandsk mobilabonnent befinner seg i et norsk 4G-nett, produseres selve 4G-tjenesten i abonnentens hjemland. Trafikken som går gjennom de norske mobilnettene er kryptert av abonnentens hjemmenett. Det samme gjelder for norske mobilabonnenter i utlandet.

Effektiv kommunikasjonskontroll på en utenlandsk abonnent i et norsk 4G-nett, ville da i praksis ha krevd at mobiloperatørene slo av kryptering på all gjestende 4G-trafikk. Dette ville samtidig betydelig svekke kommunikasjonsvernet til alle utenlandske abonnenter som gjester i norske nett, og omvendt.

Med 5G kan evnen til å gjennomføre effektiv kommunikasjonskontroll kompliseres ytterligere. Teknologisk legger 5G opp til en distribuert og skivedelt arkitektur, hvor tjenester kan produseres ulike steder, kontrolleres av tilbyder eller tredjepartsaktører, og med utgangspunkt i ulike driftsmodeller. Viktige avklaringer blir grensedragningen mellom tilretteleggingsansvaret for tilbyder og for eventuelle tredjeparter, og hva som anses som offentlige 5G-nett og hva som må betraktes som private 5G-nett.

Tillit forutsetter både effektiv kriminalitetsbekjempelse og et effektivt kommunikasjonsvern, og det vil framover være viktig å få en utvikling i nett og tjenester som ivaretar begge hensynene.

Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

I juni 2020 vedtok Stortinget ny lov om Etterretningstjenesten. Loven gir E-tjenesten mulighet til å innhente grenseoverskridende elektronisk kommunikasjon som passerer Norges grenser. Loven bygger på anbefalinger fra Lysne II-utvalgets utredning «Digitalt grenseforsvar» fra 2016, men avviker også fra anbefalingene på noen områder.

E-tjenesten får med dette nye digitale virkemidler som skal bidra til å sikre samfunnet og våre verdier mot trusler utenfra. På en annen side er kritikere av loven bekymret for om menneskeretter og personvernet ivaretas godt nok. Som med kommunikasjonskontroll omtalt over, er også dette et tillits-dilemma. I loven søkes dette balansert gjennom en rekke betingelser og kontrollmekanismer for innhenting, bruk og etterkontroll.

Personlig sikring av kommunikasjon

Politiets lovbestemte tilgang til informasjon og kommunikasjon etter ekomloven retter seg mot ekomtilbyderne og kommunikasjonen de kontrollerer i sine nett. Imidlertid skjer mer og mer av kommunikasjonen mellom personer i tjenester levert av innholdsleverandører «over-the-top». Fra en ekomtilbyder sitt ståsted er slike tjenester som oftest ende-til-ende krypterte datastrømmer, hvor tilbyder ikke har

mulighet til å gi politiet tilgang til det ukrypterte innholdet.

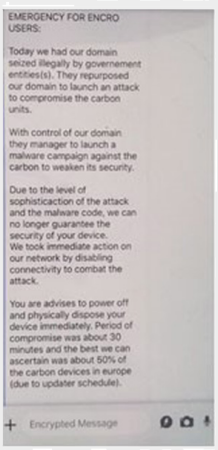
En ser også en fremvekst av løsninger i form av tjenester, eller modifiserte mobiltelefoner, som nokså utilslørt har som formål å unndra seg politiets mulighet for avlytting.

Det er ikke bare kriminelle som finner beskyttelsen i ekomnettene utilstrekkelig for sitt behov. *Signal* er en applikasjon som gjør det mulig å kommunisere kryptert ende-til-ende, og som er populær blant journalister, forskere, aktivister og andre grupper som ønsker å sikre seg mot avlytting. Men slike applikasjoner anses også relevante for myndigheter. Blant annet instruerte EU-kommisjonen i februar sin stab å bruke Signal for å beskytte intern kommunikasjon mot datalekkasjer og hacking.

I juli 2020 meldte Europol om et stort antall arrestasjoner og beslag av narkotika, våpen og kontanter i organiserte kriminelle miljøer, primært i Frankrike, Nederland og Storbritannia, men også i Sverige og Norge. 16 Arrestasjonene var resultatet av en omfattende europeisk etterforskning, der krypterte kommunikasjonstjenester og modifiserte telefoner fra EncroChat var helt sentrale.

Frem til begynnelsen av 2020 var EncroChat blant de største tilbyderne av krypterte kommunikasjonstjenester i Europa. Tjenesten var utbredt i kriminelle miljøer. Telefoner fra EncroChat ble solgt i organiserte kriminelle miljøer med garanti om komplett anonymitet og konfidensialitet. Telefoner og SIM-kort var ikke knyttet til en eier eller disponent, og salget var organisert for å hindre sporbarhet. Telefonene var modifisert og kamera, mikrofon, GNSS-sender/mottaker og USB-port var fjernet.

Politimyndighetene utførte et skadevareangrep mot tjenesten i 2020, som ga tilgang til innholdet i kommunikasjonen hos en stor andel av EncroChats brukere. Politiet hadde tilgang fra mars til midten av juni 2020, da EncroChat oppdaget at tjenesten var kompromittert og stengte ned sine systemer. Før tjenesten ble stengt varslet EncroChat sine brukere om at tjenesten ikke lenger var sikker.



Illustrasjon av EncroChats skjulte brukergrensesnitt og skjermdump av meldingen som ble sendt fra EncroChat for å varsle brukerne om at systemet var kompromittert.

[16] *Pressemelding:* *Pressemelding: https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe*

3.3 KOMPLEKSE VERDI- OG LEVERANDØRKJEDER

Verdi- og leverandørkjedene som ligger til grunn for å produsere de ekomtjenestene som utgjør den digitale grunnmuren blir stadig mer komplekse. For å kunne opprettholde brukernes og samfunnets tillit til egne nett og tjenester, må ekomtilbyderne på sin side ha kontroll på og etablere nødvendig tillit i egne verdi- og leverandørkjeder.

Forenkling eller kompleksitetsforskyvning?

Et fellestrekk med utvidelsen av verdi- og leverandørkjedene er at kompleksiteten gjerne «forskyves» fra ett sted i verdikjeden til et annet. Dette skjer for eksempel gjennom å virtualisere, flytte til skyen, og ved i økende grad å automatisere styrings- og kontrolloppgaver.

Blant annet legger virtualiseringen til rette for skivedeling i de fremtidige 5G-nettene, som muliggjør flere logiske nett med ulike egenskaper, innenfor samme fysiske nett. Virtualiseringen er i stor grad drevet av ønsket om å redusere kostnader, øke fleksibiliteten og skalerbarheten på tjenestene, og å redusere tiden for å bringe nye tjenester til markedet.

På den ene side fører denne utviklingen til en forenkling. For eksempel erstattes spesialisert maskinvare med hyllevareutstyr, og ekomspesifikke protokoller med standard IT-protokoller. På den annen side blir ikke den samlede kompleksiteten i verdikjeden mindre. I noen tilfeller er det snakk om nye lag med komponenter og underleverandører. I andre tilfeller vil deler av produksjonen av ekomtjenester forskyves til et nytt nivå.

Verdikjedene strekker seg over landegrenser

Utviklingen beskrevet over, bidrar også i økende grad til at verdi- og leverandørkjedene strekker seg over landegrensene. I 2018 og 2019 deltok Nkom i en arbeidsgruppe ledet av Professor Olav Lysne, der det ble rettet fokus på komplekse verdikjeder og betydningen dette har for risikostyring. Rapporten [17] fra arbeidsgruppen peker på tre hovedårsaker til at de digitale verdikjedene får forgreininger ut av landet.

For det første anses internett som den viktigste infrastrukturen i dagens ekomtjenester, og selve arkitekturen til internett gjør nasjonal kontroll vanskelig. En hovedruter eller lisenstjener plassert i utlandet kan påvirke om en tjeneste er tilgjengelig i Norge. For det andre er det lite elektronikk og programvare som i sin helhet produseres i Norge, med norskproduserte verktøy. For det tredje bidrar beslutninger om kjøp av for eksempel driftstjenester eller skytjenester fra utlandet, til at deler av verdikjeden underlegges andre staters jurisdiksjon.

3.4 AVHENGIGHET TIL OG UTNYTTELSE AV TRÅDLØS KOMMUNIKASJON

I transportnettene har fiber blitt den helt dominerende teknologien. Samtidig går utviklingen mot stadig mer trådløs kommunikasjon. Selv om vi har fiber frem til husveggen, kommuniserer både menneskene, og tingene, i økende grad via trådløs kommunikasjon.

Trådløst bredbånd som erstatning for kobber

Kobbernettet som i hundre år har vært viktig for fasttelefoni og etter hvert bredbånd, tas nå gradvis ut av bruk og erstattes med andre mer moderne løsninger. I mange tilfeller er dette fiber. I noen områder, der det ikke er kostnadssvarende med fiberfremføring til den enkelte husstand, vil kobberkabler erstattes av trådløse bredbåndsløsninger basert på mobilnettene.

Både Telenor, Telia og senest NextGenTel (via Telia-nettet), tilbyr nå slike løsninger. Abonnentsvilkårene skal tilsvare faste bredbåndsløsninger, med høy båndbredde og datapakker som skal være tilstrekkelig dimensjonert for å håndtere normalt «hjemmeforbruk». Trådløst bredbånd er et forholdsvis nytt produkt, og det gjenstår å se hvilken rolle dette produktet vil få som alternativ til fast aksess de kommende årene.

[17] «Risikostyring i digitale verdikjeder - rapport fra en arbeidsgruppe ledet av professor Olav Lysne», DSB, 2020

Massiv vekst i IoT

Utbredelsen av Internet of Things (IoT) vil stå sentralt i den videre digitaliseringen av samfunnet. Utviklingspotensialet er stort og legger til rette for nye bruksområder i flere bransjer og sektorer. Blant annet har Oslo Sporveier besluttet å erstatte sitt gamle signalanlegg med en løsning som skal basere seg på Telias mobilnett. Den samme infrastrukturen som passasjerene surfer på i morgenrushet skal dermed også bringe togene fram trygt og i rute. Dette er ett eksempel på en forventet økt kritisk bruk av mobilnettene.

I tillegg til nye IoT-anvendelser basert på 4G- og 5G-teknologien, er det også en fremvekst av løsninger basert på fribruksfrekvenser. En populær kommunikasjonsprotokoll for IoT er LoRaWAN, som er tilrettelagt særskilt for anvendelser som sensornettverk, industristyring, smarthjem, smartbyer. For eksempel inngår LoRaWAN-baserte løsninger i en del «smartby»-prosjekter, blant annet i Stavanger.

Wi-Fi er fortsatt normalen for trådløs kommunikasjon innendørs, både for ordinær datakommunikasjon og for ulike IoT-anvendelser i hjemmet. Protokoller som benytter fribruksfrekvenser, som Wi-Fi og LoRaWAN er attraktive da de ofte er billigere enn løsninger basert på mobilnettene. Imidlertid kan kvaliteten og sikkerheten på dette utstyret variere veldig.

Etter hvert ventes de ulike IoT-løsningene å inngå i sentrale deler av verdikjeden til stadig flere kritiske funksjoner. For de som tar i bruk IoT-løsninger er det derfor viktig å være bevisst på at også sårbarhetskarakteristikkene kan være svært forskjellige for de ulike kommunikasjonsprotokollene og løsningene.

Satellittbaserte navigasjonssystemer

GNSS [18] er en samlebetegnelse på satellittbaserte systemer for navigasjon, posisjonsbestemmelse og tidsbestemmelse. Det mest utbredte systemet i dag er det amerikanske GPS, men det eksisterer også tilsvarende europeiske (Galileo), russiske (GLONASS) og kinesiske (BeiDou) systemer.

[18] *Global Navigation Satellite System*

Foto: Alf S. Aanonsen/Nkom

GNSS benyttes innenfor en rekke sektorer, inkludert Forsvaret, luftfarten, elektronisk kommunikasjon, kraftforsyning, petroleumsindustrien, anleggsbransjen og i landbruket.

I økende grad inngår GNSS som en sentral del av verdikjeden i samfunnskritiske funksjoner. Signalene som benyttes i GNSS kommer fra satellitter i baner ca. 20.000 kilometer over bakken og er dermed meget svake ved ankomst til jordoverflaten. GNSS er derfor spesielt sårbart for jamming (støy) eller spoofing (manipulering).

Som kilde til nøyaktig tid og takt i 4G-mobilnettene benyttes i dag enten GNSS (via mottakere på basestasjoner) eller atomklokker (via fibernettet), eller en kombinasjon av disse to. Også en del av småeffektssenderne i DAB radionettet er avhengige av synkronisering via GPS. Disse senderne utgjør ca. 5% av befolkningsdekningen. I 5G stilles det svært høye krav til nøyaktighet i synkroniseringen. Valg av synkroniseringsmetode vil avhenge av utstyrsleverandørenes løsninger og hvilke fiber- og klokkeinfrastruktur mobiloperatørene har.

Satellittbaserte bredbåndssystemer

Markedet for satellittkommunikasjonstjenester er i utvikling mot høyere ytelser og lavere priser. Den hittil dominerende tekniske løsningen med satellitter i geostasjonære baner, blir nå utfordret med nye lavbaneinitiativer.

Det finnes allerede i dag veletablerte lavbanesystemer som tilbyr datatrafikk og taletjenester, som Globalstar og Iridium. Men det er også nye initiativer på gang, hvor Starlink er det mest fremtredende.

Nye lavbanesystemer kan, om de lykkes, få en rolle både som en selvstendig alternativ kommunikasjonsløsning til landbaserte mobilnett. Men de kan også få en rolle som en integrert del av andre kommunikasjonsløsninger.

For eksempel har Nødnett i dag transportable basestasjoner med satellittbasert transmisjon og strømaggregat, som gjør at basestasjonene kan settes ut i terrenget uten å måtte knyttes til bakkebasert infrastruktur.

I de kommersielle mobilnettene er slike satellittbaserte beredskapsløsninger mindre aktuelle i dag, grunnet forholdsvis høy pris, lav kapasitet og høy forsinkelse. Dette kan imidlertid endre seg med de nye lavbanesystemene da disse er designet for å levere betydelig høyere kapasitet og lavere tidsforsinkelse enn de eksisterende systemene.

Dette avhenger av at satellittoperatørene evner å rulle ut tjenestene sine i et stort nok geografisk omfang og til de lave tjenesteprisene som er forespeilet. Det er også usikkerhet rundt prisnivået på terminalene som er under utvikling.

Et av de mest fremtredende initiativene nye bredbåndssatellitt-initiativene er Starlink, som amerikanske SpaceX og Elon Musk står bak. Starlink-konstellasjonen skal etter planen bestå av så mange som 12 000 satellitter i lavbane. Per 15. september 2020 var 775 satellitter skutt opp. Det planlegges videre for oppskytinger annenhver uke med 60 satellitter i hver oppskyting.

Foto: Anders Martinsen/Nkom

4

SENTRALE RISIKOOMRÅDER FOR DE KOMMENDE ÅRENE

De årlige EkomROS-rapportene kompletterer hverandre slik at de over noen år til sammen fanger opp de vesentlige og overordnede sikkerhetsutfordringene i sektoren.

Ekomloven stiller krav til at ekomnett- og tjenester skal være bygget med forsvarlig sikkerhet for brukerne i fred, krise og krig. Ved vurdering av risiko må aktørene underlagt loven ta hensyn til både utilsiktede og tilsiktede hendelser, i hele krisespekteret. I tillegg må det tas hensyn til alle sikkerhetsaspekter, både tilgjengelighet, integritet og konfidensialitet.

EkomROS legger først og fremst vekt på å skape oppmerksomhet om aktuelle risikoområder innenfor ekomsektoren. Det er deretter den enkelte ekomtilbyders selvstendige ansvar å gjennomføre konkrete risikovurderinger for egen virksomhet, og iverksette nødvendige risikoreduserende tiltak.

4.1 STRØMBRUDD OG SKADER PÅ INFRASTRUKTUR MÅ FORTSATT FORVENTES

Til grunn for all elektronisk kommunikasjon ligger den *fysiske* ekominfrastrukturen, som fiberkabler, basestasjoner, og sentraler og datasentre med nettverksutstyr og servere. Videre er ekominfrastrukturen avhengig av annen kritisk støtteinfrastruktur som strømforsyning og kjøling.

Den fysiske infrastrukturen har gjennom årene blitt gradvis forsterket. Krav til fysisk sikring, redundans og reservestrømberedskap følger av krav både i ekomloven og sikkerhetsloven. Videre bidrar Nkom med tilskuddsmidler for å gjennomføre tiltak som skal bidra til å sikre nasjonale behov til sikkerhet og beredskap utover det tilbyderne plikter å gjøre på egenhånd.

De siste tre-fire årene har vi sett en nedgang av større og omfattende utfallshendelser som følge av skader på fysisk infrastruktur. Dette skyldes en kombinasjon av et målrettet arbeid i sektoren for å styrke den fysiske sikkerheten, redundansen og beredskapen, og at det de siste årene har vært færre ekstremvær og andre store, alvorlige naturhendelser.

Imidlertid tilsier klimaprognosene at vi i årene fremover må forvente mer ekstremvær og alvorlige naturhendelser. Dette kan være ekstrem vind, ekstrem nedbør med påfølgende skred, snø/ising-problematikk og flom i elver og vassdrag. Men også langvarige tørkeperioder med påfølgende skog- og utmarksbranner må forventes.

Det pågående arbeidet med å forsterke den fysiske ekominfrastrukturen må derfor opprettholdes og videreføres i årene fremover. Særlig ser Nkom behov for tiltak som styrker «kanten» av ekomnettene, som regional- og aksessnett og mobilbasestasjoner. Dette er den delen av ekominfrastrukturen som er mest sårbar for påkjenninger fra naturen.

4.2 SIKRING AV KJERNEFUNKSJONER PÅ INTERNETT BLIR STADIG VIKTIGERE

Nedstengingen av samfunnet 12. mars 2020 førte til økt trafikk og endret trafikkmønster på internett. Ekomtilbyderne håndterte denne økningen på en tilfredsstillende måte. Det oppsto i liten grad trafikkork og problemer i nettverkslaget på internett. En tilbyder opplevde den 18. mars, og igjen den 30. mars, en DNS-feil som påvirket bredbåndskundene på fastnett på Sørlandet og Vestlandet over en periode på til sammen fire til fem timer. Ut over dette sammenfalt ikke nedstengingen av samfunnet

med større tekniske feilsituasjoner på kritiske internett-kjernefunksjoner som samtrafikk og trafikkstyring mellom nett (BGP-ruting), domeneoppslag (DNS), tidstjenere (NPT).

Mange sårbarheter og utfordringer knyttet til internett er grenseoverskridende i sin natur. Når en av verdens største teleoperatører fikk problemer med rutingen i sitt internasjonale nett i august 2020, rammet dette internett-tjenester bredt i både USA og i Europa, inkludert Norge. Hendelsen viser hvordan en «liten feil» i en kompleks transnasjonal digital verdikjede kan forplante seg, og også alvorlig påvirke tilgang til tjenester i Norge.

Hendelsen illustrerer også viktigheten av å opprettholde god diversitet på samtrafikk mot internasjonale nett, og samtidig ha god beredskap og evne til rask omstilling.

Tilsvarende er det viktig å etablere god diversitet og kapasitet på samtrafikken på både nasjonalt og regionalt nivå. Norsk samtrafikk på internett skjer i dag hovedsakelig på samtrafikkpunkter i Oslo-området. Regionale samtrafikkpunkter blir i liten grad utnyttet.

Alvorlige uønskede hendelser som rammer trafikken mot de store samtrafikkpunktene eller de store tilbyderne, kan både føre til kapasitetsproblemer, og til at kritiske internett-kjernefunksjoner blir utilgjengelig. Slike hendelser kan være både fysiske skader, ulykker eller sabotasje, logiske feil eller målrettede digitale angrep.

Sikring av kritiske internett-kjernefunksjoner i Norge og økt diversitet på internasjonal, nasjonal og regional samtrafikk er viktige tiltak for å øke motstandsdyktigheten og autonomien i den norske delen av internett.

4.3 FORSTYRRELSER OG MANIPULERING AV TRÅDLØS KOMMUNIKASJON

Det forventes en formidabel vekst i antall enheter som skal kommunisere trådløst. Dette gjør at det blir stadig «trangere om plassen» i radiospektrumet, noe som øker sannsynligheten for utilsiktet interferens og støyproblematikk.

Samtidig forventes det at stadig flere av de trådløse anvendelsene vil være relatert til kritiske samfunnsfunksjoner. De potensielle konsekvensene av utilsiktet støy eller bevisst jamming eller spoofing blir dermed også høyere.

Hver for seg vil en interferenshendelse gjerne være av lokal og begrenset art. Men dersom problemer øker betydelig i volum vil dette svekke den generelle tilliten til kommunikasjonsløsningene.

Det samme vil gjelde for utnyttelse av sårbarheter som rammer konfidensialiteten eller integriteten på kommunikasjonen i de trådløse grensesnittene. Ikke minst vil dette gjelde for de forespeilede kritiske anvendelsene av 5G.

Regjeringens strategi [19] for posisjonsbestemmelse, navigasjon og tidsbestemmelse (PNT) beskriver sårbarheter og tiltak knyttet til GNSS. Et tiltak for å redusere sårbarheten for bortfall eller manipulering av GNSS-signaler vil være å sikre alternative jordbundne løsninger for nøyaktig PNT. I ekomnettene kan nøyaktig tid også distribueres gjennom fibernettene fra egne atomklokker.

Nkom styrker arbeidet med tilsyn og kontroll med frekvensforstyrrelser. Det pågår et samarbeid med Norsk Romsenter rundt kartlegging og håndter ing av GNSS-forstyrrelser. Nye fjernmålestasjoner etableres, og Nkom samarbeider med forskning smiljøer for å effektivisere analyse av måledata fra disse. Videre tar Nkom i bruk droner for å bistå kontroller og frekvensmålinger i lite tilgjengelige områder.

[19] *«Riktig sted til riktig tid - nasjonal strategi for posisjonsbestemmelse, navigasjon og tidsbestemmelse», Samferdselsdepartementet, 2018*

Foto: Nkom

4.4 RISIKOHÅNDTERING I KOMPLEKSE VERDI- OG LEVERANSEKJEDER I 5G

Mobiloperatørene Telia, Telenor og ICE har kommet godt i gang med utrullingen av 5G i Norge. I første omgang bygges basestasjonene ut med 5G-teknologi, som optimaliserer utnyttelsen av frekvensressursene, og gir dekning med betydelig økt kapasitet og båndbredde.

Den neste fasen av 5G-utbyggingen er moderniseringen av selve kjernenettet. Teknologien vil muliggjøre mange nye anvendelser av mobilnettene, blant annet innenfor industrien, helsesektoren og transportsektoren. Det ventes at 5G gradvis vil integreres i stadig flere kritiske samfunnsfunksjoner.

Teknologien som ligger til grunn for 5G skiller seg fra tidligere generasjoner ved at den i mye større grad tar i bruk virtualisering, skybaserte løsninger og kompleks automatisering. Dette muliggjør blant annet flere parallelle logiske mobilnett på samme fysiske nett (skivedeling) og at funksjoner og tjenesteproduksjon som tidligere var sentralisert, også kan distribueres og flyttes nærmere brukerne. 5G åpner også for en tettere integrasjon av 3. partsaktører i mye større grad enn tidligere generasjoner.

Kompleksitetsveksten i verdi- og leveransekjedene i 5G-økosystemet ventes å føre til vesentlige endringer i risikobildet. Verdi- og leveransekjedene, og hvordan disse strekker seg over landegrenser, må kartlegges. Potensielle angrepsinnganger og kilder til utilsiktede feil må identifiseres. I tillegg til de store og sentrale utstyrsleverandørene, bør også små og mindre «betydningsfulle» underleverandører vies oppmerksomhet da disse kan representere sårbarheter som lettere går «under radaren».

Ekommyndigheten må på sin side sørge for oppdaterte og relevante krav knyttet til sikkerhet i 5G. Nkom følger også den internasjonale reguleringen på feltet, blant annet gjennom ENISA og BEREC. Blant annet publiserte EU-organet NIS Cooperation Group [20] tidlig i 2020 en «5G Cybersecurity Toolbox» som utgjør retningslinjene EU-kommisjonen støtter seg på i arbeidet med 5G-sikkerhet.

[20] *Network and Information Security Cooperation Group ble etablert med NIS-direktivet*

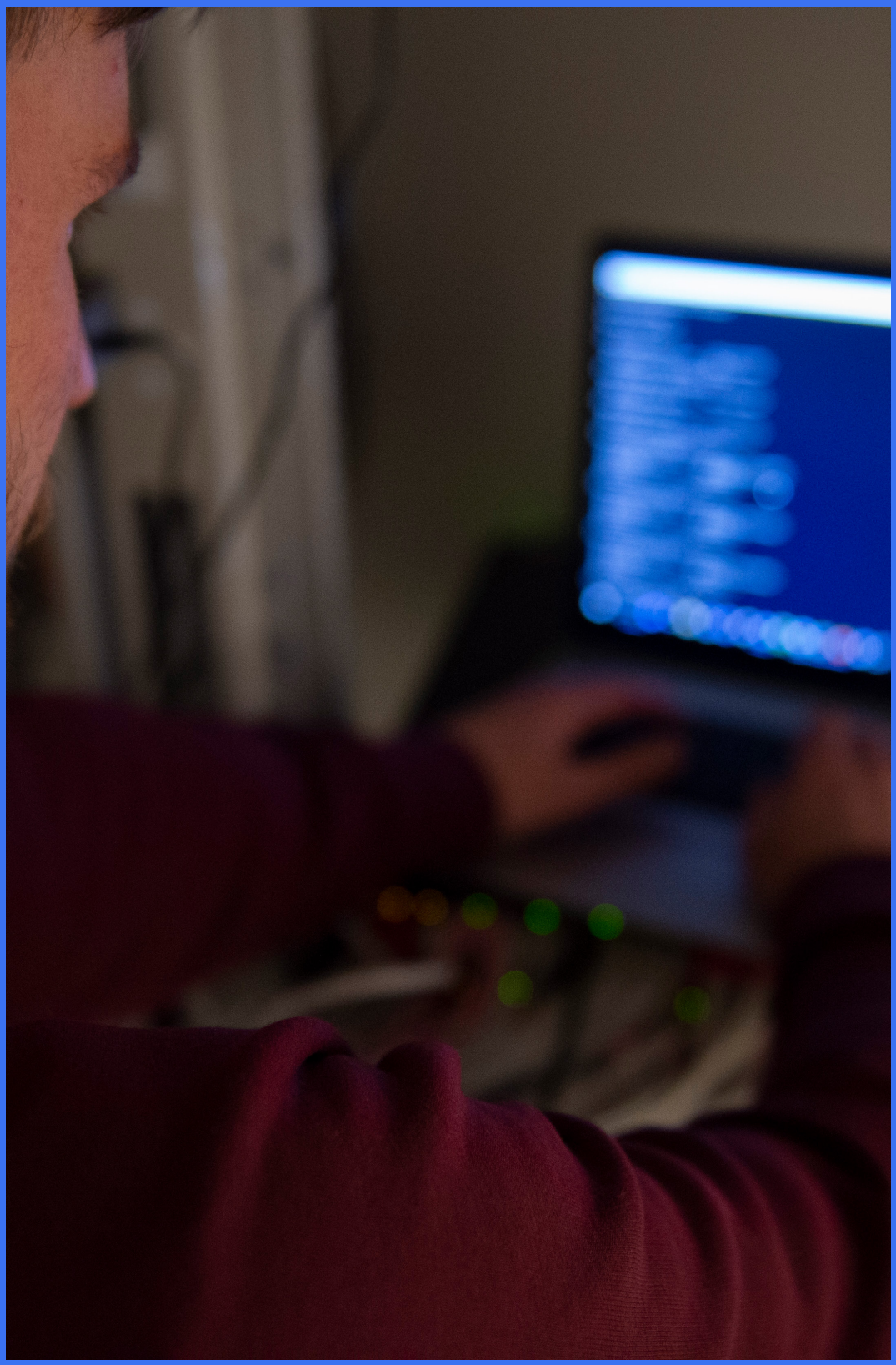


Foto: Anders Martinsen/Nkom

5

RISIKOHÅNDTERING

5.1 MYNDIGHETENS ULIKE ROLLER

Nkom har både en tilsyns-, veilednings- og forvaltningsrolle i sikkerhetsarbeidet i sektoren. Risikobasert tilsyn gjennomføres både etter lov om elektronisk kommunikasjon og etter sikkerhetsloven. Nkom har ilagt overtredelsesgebyr i flere sikkerhetsrelaterte saker de siste årene.

Veiledning og samarbeid med bransjeaktører og andre myndigheter utgjør en svært viktig del av risikohåndteringen. Ekomsikkerhetsforum, som kobler sammen sikkerhetsmyndighetene og tilbyderne underlagt sikkerhetsloven, og andre sikkerhets- og beredskapsfora er viktige arenaer for gradert informasjonsutveksling mellom myndighetene og tilbyderne.

Nkoms forvaltningsrolle innebærer blant annet videreutvikling av det nasjonale lov- og forskriftsarbeidet, oppfølging av internasjonale aktiviteter innenfor standardisering og regelverksutvikling.

Nå arbeides det blant annet med å utpeke skjermingsverdige objekter og infrastrukturer som skal danne utgangspunkt for tilbydernes sikringstiltak i henhold til kravene i sikkerhetsloven som trådte i kraft i 2019.

5.2 AKTUELLE TILTAK

Nkom fortsetter arbeidet med myndighetsfinansierte tiltak for å oppfylle nasjonale behov for sikkerhet og beredskap. Blant annet bidrar «Forsterket ekom»-programmet årlig med statlig finansiering til å styrke strategisk viktige basestasjoner i hver kommune med reservestrøm og dobbel transmisjon.

I 2020 planlegges det utbygging i 10 kommuner i Finnmark. Også andre tiltak er under planlegging for å styrke transportnettinfrastrukturen i Finnmark.

I juli 2020 inngikk Nkom avtale med Telia Carrier om å bygge ut et nytt sjøfibersamband mellom Kristiansand og Esbjerg, Danmark, for å legge til rette for økt diversitet på rutingen av internett-trafikk og annen offentlig ekomtrafikk mellom Norge og utlandet. Forbindelsen skal være klar fra 2022. Det planlegges også tiltak for å styrke samtrafikkpunkter som skal bidra til økt diversitet og sikkerhet på internetttrafikken.

Nkom EkomCERT samarbeider tett med sikkerhetsmiljøene hos de norske ekomtilbyderne, i tillegg til Nasjonalt cybersikkehetssenter og andre sektorresponsmiljøer som KraftCERT og Nordic Financial CERT.

EkomCERT mottar daglig store menger informasjon som analyseres og sammenholdes med aktuelt situasjonsbilde. I 2020 lanseres en ny portalløsning for å effektivisere informasjonsdelingen med tilbyderne i sektoren.

Besøksadresse:
Nygård 1, Lillesand

Postadresse:
Postboks 93, 4791 Lillesand

Tlf: 22 82 46 00

nkom.no