Nkom ROS

Nasjonal kommunikasjonsmyndighets risiko- og sårbarhetsanalyse

2026



Nasjonal kommunikasjonsmyndighet

SAMMENDRAG

Elektronisk kommunikasjon er en kritisk del av totalforsvaret, og ekomsektoren står overfor et sammensatt og skjerpet risikobilde. Hybride trusler, som kombinerer politiske, økonomiske og digitale virkemidler, utgjør en av de mest komplekse utfordringene for sektoren i Norge. Slike trusler kan utnytte sårbarheter i både fysisk og digital infrastruktur og utfordrer etablerte sikkerhets- og beredskapsmodeller.

Datasenternæringen er en kritisk infrastruktur som i 2025 ble underlagt ekomloven. Dette tydeliggjør krav til forsvarlig sikkerhet og styrker det samlede tilsyns- og beredskapsregimet. Samtidig er datasentersektoren mindre moden på sikkerhetsområdet enn den etablerte ekomsektoren, som over tid har vært underlagt omfattende regulering. Dette kan påvirke sektorens evne til å håndtere langvarige og sammensatte hendelser høyere opp i krisespennet, og understreker behovet for videre utvikling av beredskap, kompetanse og øving.

Cybertrusselen vurderes fortsatt som den mest alvorlige trusselen mot ekominfrastrukturen, med stort skadepotensial. Cyberoperasjoner spenner fra støyende og kapasitetskrevende angrep til skjulte og langvarige operasjoner rettet mot kritisk infrastruktur. Samtidig bidrar økt bruk av kunstig intelligens til mer sofistikerte angrep og lavere terskel for gjennomføring. Innsidetrusselen er også økende og representerer en særlig alvorlig risiko, ettersom innsideren allerede har tilgang til systemer og kan omgå etablerte sikkerhetsmekanismer.

Ekomsektoren er samtidig preget av strukturelle sårbarheter. Planlagt arbeid i fast- og mobilnett skjer i stadig mer komplekse miljøer med mange leverandører og tett integrerte systemer. Dette gjør det krevende å ha full oversikt over avhengigheter og konsekvenser av endringer. Feil kan raskt forplante seg og gi uforutsette ringvirkninger, ofte forsterket av mangelfulle risikovurderinger, utilstrekkelig endringshåndtering og fragmentert ansvar i leverandørkjedene.

Avhengigheter i verdikjeder fremstår som en sentral sårbarhet, særlig i lys av økt bruk av internasjonale leverandører og tjenester utenfor norsk jurisdiksjon. Dette kan gi økt risiko for bortfall, påvirkning eller uønsket tilgang. Det er viktig at leverandører har god oversikt over og kontroll på sikkerhetsprosessene, ikke bare i egen virksomhet, men også hos sine underleverandører. Verdikjedene er ofte komplekse, og svakheter hos en underleverandør kan utgjøre en inngangsport for sikkerhetsbrudd. Manglende innsikt i eller oppfølging av underleverandørers sikkerhetsnivå kan dermed svekke den samlede sikkerheten betydelig. For å redusere risiko er det derfor avgjørende med tydelige krav, oppfølging og kontinuerlig vurdering av sikkerhetsarbeidet i hele leverandørkjeden.

Sektoren er også avhengig av presis posisjonering, navigasjon og tid. Økende forekomst av GNSS-forstyrrelser representerer en konkret risiko for både ekomtjenester og andre samfunnskritiske funksjoner.

Naturhendelser kan utgjøre en vesentlig trussel mot ekomsektoren. Transmisjons- og strømbrudd er blant de vanligste årsakene til utfall, og utgjør om lag tre fjerdedeler av registrerte hendelser. Ekstremvær som storm, kraftig nedbør og flom kan føre til samtidige bortfall av strøm og transmisjon over større geografiske områder. Selv om de fleste hendelser har lokale eller regionale konsekvenser, kan utfall i transportnettet gi betydelige samfunnsmessige konsekvenser.

Den sikkerhetspolitiske situasjonen er alvorlig og preget av økt spenning. Statlige aktører kan utgjøre en trussel gjennom ulike virkemidler, herunder cyberoperasjoner, påvirkningsoperasjoner og desinformasjon. Samtidig understrekes behovet for en kunnskapsbasert tilnærming til trusselbildet. I tillegg bidrar et stort omfang av digital svindel til å kunne svekke tilliten til digitale tjenester. Disse tjenestene er en grunnleggende forutsetning for at samfunnet skal kunne fungere i fred, krise og krig.

Kartlegginger gjennomført i 2025 har synliggjort utfordringer knyttet til fysisk robusthet og beskyttelse av kritisk ekominfrastruktur. Dette har aktualisert behovet for mer ensartede krav og praksis for etablering, sikring og vedlikehold av infrastruktur. Som oppfølging pågår det arbeid med å utvikle en bransjestandard som skal bidra til redusert sårbarhet og økt robusthet i den digitale grunnmuren. I tillegg identifiserer denne rapporten en rekke risikoreduserende tiltak knyttet til de farene, truslene og sårbarhetene som er beskrevet. Målet er å styrke sektorens sikkerhet, beredskap pg motstandskraft.

Samlet sett peker rapporten på et gap mellom dagens sikkerhetsnivå i sektoren og det som kreves i en mer krevende sikkerhetspolitisk situasjon. For å møte dette må myndigheter, næringsliv og øvrige aktører gjøre en felles innsats for å styrke robustheten i ekomsektoren og sikre at samfunnet kan opprettholde samfunnskritiske funksjoner i hele krisespennet.

Nasjonal kommunikasjons-myndighet



Foto: Nkom

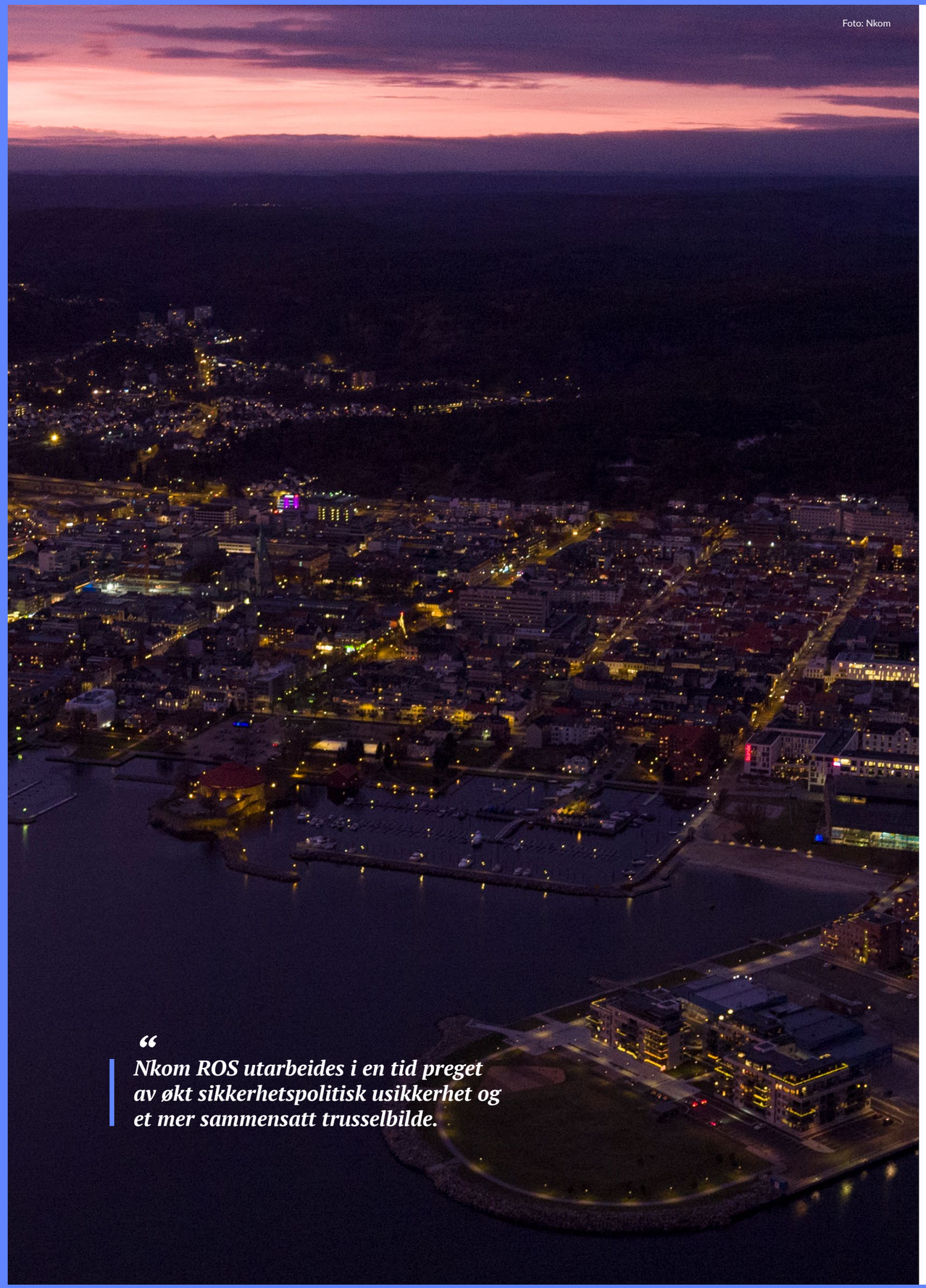
Innhold

SAMMENDRAG 2

1 INNLEDNING OG BAKTEPPE FOR NKOMROS 2026 7
1.1 Rapporterte hendelser om utfall i ekom 2025 8
1.2 Sentrale begreper i rapporten 10

2 FARER, TRUSLER OG SÅRBARHETER I SEKTOREN 15
2.1 Statlige trusler 15
2.2 Sårbarheter i cyberdomenet 20
2.3 Posisjonsbestemmelse, Navigasjon og Tidsbestemmelse (PNT) 27
2.4 Digital svindel 32
2.5 Verdi og leverandørkjeder 36
2.6 Planlagt arbeid 41
2.7 Naturhendelser 47

3 NKOMS EGENBEREDSKAPSRÅD OG OPPSUMMERING AV ANBEFALTE TILTAK 53



> *Nkom ROS utarbeides i en tid preget av økt sikkerhetspolitisk usikkerhet og et mer sammensatt trusselbilde.*

1 INNLEDNING OG BAKTEPPE FOR NKOMROS 2026

Som sektoransvarlig myndighet skal Nasjonal Kommunikasjonsmyndighet (Nkom) bidra til et likeverdig, sikkert og robust tilbud av post- og ekomtjenester over hele landet. Nkom har et særskilt ansvar for sikkerhet og beredskap i elektroniske kommunikasjonsnett og -tjenester, herunder oppfølging av digitale angrep, fysiske trusler og belastninger som følge av naturhendelser. Dette omfatter også krav til sikkerhet i datasentre, samt en aktiv rolle i utviklingen av nytt nødnett og beredskap ved ekomhendelser. Nkom er også ansvarlig tilsynsmyndighet for postsektoren i Norge. Posttjenester utgjør en viktig del av samfunnets grunnleggende infrastruktur og har betydning for nasjonal beredskap. Postsektoren er ikke behandlet som et eget tema i årets NkomROS, men vil bli vurdert nærmere dersom Nkom får delegert ytterligere ansvar på området.

NkomROS må ses i sammenheng med Nkoms øvrige arbeid på området. I 2025 gjennomførte Nkom en regional risiko- og sårbarhetsanalyse[1] for Innlandet og Buskerud, og utarbeidet en tilstandsvurdering for digital infrastruktur i ekomsektoren. Samlet bidrar disse arbeidene til å gi et bredere bilde av sektorens robusthet og evne til å opprettholde funksjon og kontinuitet.

Nkom ROS utarbeides i en tid preget av økt sikkerhetspolitisk usikkerhet og et mer sammensatt trusselbilde. Den internasjonale utviklingen, med skjerpet stormaktsrivalisering og økende konfliktnivå, bidrar til et uforutsigbart risikobilde som også påvirker norske interesser og samfunnssikkerheten.

I totalforsvarsåret 2026 rettes det særskilt oppmerksomhet mot samvirket mellom sivile og militære aktører. Totalforsvaret bygger på forutsetningen om at samfunnets samlede ressurser skal kunne utnyttes koordinert ved kriser, væpnet konflikt og krig. Dette stiller økte krav til robuste og sikre sivile infrastrukturer som kan understøtte både samfunnets grunnleggende funksjoner og militær operativ evne. Elektronisk kommunikasjon (ekom) utgjør en grunnleggende forutsetning for dette samvirket. Sammen med datasentre, post og digitale tillitstjenester, danner ekom grunnlaget for sikker identifisering, digital samhandling, daglig drift og krisehåndtering. Ekom er dermed en kritisk bærebjelke i hele krisespennet fra fred til krig, og en forutsetning for effektiv ledelse, informasjonsdeling og operativ koordinering.

Samtidig preges dagens risikobilde av sammensatte trusler og glidende overganger mellom fred, krise og konflikt. Hybride virkemidler, herunder cyberangrep, fysisk sabotasje og påvirkningsoperasjoner, kan utnytte sårbarheter i både fysisk og digital infrastruktur. I dette bildet blir ekom både et mål for uønskede hendelser og en avgjørende forutsetning for å håndtere dem.

De overordnede vurderingene i denne analysen må også ses i sammenheng med de nasjonale trussel- og risikovurderingene fra EOS-tjenestene. Etterretningstjenestens rapport *Fokus 2026* peker på at stormaktene prioriterer egne interesser for rask vinning, at den sterkestes rett får større gjennomslag, og at internasjonalt samarbeid og etablerte institusjoner svekkes. Politiets sikkerhetstjenestes *Nasjonal trusselvurdering 2026* fremhever at Norge befinner seg i den mest alvorlige sikkerhetspolitiske situasjonen siden andre verdenskrig. Fremmede statlige aktører tar i bruk sammensatte virkemidler i Norge for å undergrave vår motstandsdyktighet. Nasjonal sikkerhetsmyndighets *Risiko 2026* understreker

samtidig at dette skjer i et sammensatt risikobilde, hvor teknologisk utvikling, avhengigheter og sårbarheter i samfunnskritisk infrastruktur øker behovet for systematisk forebyggende sikkerhetsarbeid. Samlet gir disse vurderingene et situasjonsbilde som danner et viktig bakteppe for *Nkom ROS 2026*.

Utviklingen innen teknologi og digitalisering har gitt betydelige gevinster i form av effektivitet og tilgjengelighet, men har også ført til økt kompleksitet og nye avhengigheter. Dette forsterker behovet for en helhetlig tilnærming til risiko og sårbarhet, der ekomsektoren vurderes i sammenheng med øvrige deler av totalforsvaret.

Nkoms ROS 2026 har som mål å gi et oppdatert kunnskapsgrunnlag om risiko og sårbarheter i sektoren, og å bidra til økt bevissthet og bedre grunnlag for prioriteringer og tiltak hos myndigheter og aktører. Målgruppen er Digitaliserings- og forvaltningsdepartementet, øvrige departementer og myndigheter, stats-forvaltere, ekomtilbydere og andre relevante aktører.

1.1 RAPPORTERTE HENDELSER OM UTFALL I EKOM 2025

Transmisjonsbrudd og strømbrudd er fortsatt blant de vanligste årsakene til brudd i elektroniske kommunikasjonstjenester på fastlandet i Norge. Hendelser som er innrapportert til Nkom i 2025 viser at dette utgjør om lag tre fjerdedeler av registrerte utfall i tilbydernes ekomnett.

Naturhendelser som storm, kraftig nedbør, skred og flom fører jevnlig til skader på infrastruktur, og i mange tilfeller er det bortfall av strøm som utløser selve transmisjonsbruddet. Ved ekstremvær kan bortfall av transmisjon og strøm oppstå samtidig og ramme flere lokasjoner over store geografiske områder.

Hva gjør ekomnettene sårbare?

På landsbasis er ekomnettene sårbare for både tekniske feil, naturhendelser og tilsiktede handlinger. Sårbarhetene varierer geografisk. I Nord-Norge er svak redundans i lands- og regionnett en utfordring, mens region- og lokalnett flere steder i Sør-Norge kan være utsatt for feil som isolerer lokalsamfunn. Ekominfrastrukturen er mange steder lett tilgjengelig og eksponert, samtidig som kraftforsyning og begrenset reservestrømkapasitet utgjør viktige avhengigheter. Geografi, værforhold og andre naturgitte faktorer kan forsterke konsekvensene av bortfall. I tillegg kan mangelfull informasjonsdeling og komplekse avhengigheter mellom tilbydere gjøre håndtering og gjenoppretting av tjenester mer krevende ved større hendelser.


Foto: Nkom

Konsekvensene av ekomutfall varierer, men de fleste hendelsene får lokale eller regionale virkninger. Hendelser i transportnettet gir imidlertid større konsekvenser enn utfall i aksessnettet, blant annet som følge av høyere trafikkvolum og flere berørte tjenester, selv om sannsynligheten for slike hendelser er lavere grunnet høyere robusthet og flere risikoreduserende tiltak.

Programvarefeil står for flere av de mest omfattende hendelsene. Slike feil er ikke nødvendigvis geografisk avgrenset og kan føre til landsdekkende bortfall av tjenester. Maskinvarefeil har også forårsaket enkelte større utfall med betydelige konsekvenser.

Andre årsaker til hendelser er blant annet arbeid i og nær ekomnett, maskinvarefeil og menneskelige feil ved drift og endringer i nettene. Samlet sett dominerer transmisjonsbrudd og strømbrudd fortsatt hendelsesbildet.

Hva kan skje når digital infrastruktur svikter?

Svikt i digital infrastruktur kan føre til bortfall av nødkommunikasjon, redusert tilgang til helse- og beredskapstjenester, påvirkning på lufttrafikken, isolasjon av lokalsamfunn og utilgjengelige digitale tjenester. Konsekvensene kan ramme både enkeltpersoner, virksomheter og samfunnskritiske funksjoner.

[1] Regionale risiko- og sårbarhetsanalyser - Nkom

1.2 SENTRALE BEGREPER I RAPPORTEN

I denne rapporten brukes flere begreper innen elektroniske kommunikasjonssystemer og andre teknologiske områder. Forklaringer på noen av de viktigste er:

Forsvarlig sikkerhet handler om evnen til å stå imot hendelser som medfører eller kan medføre brudd på tilgjengelighet, autentisitet, integritet eller konfidensialitet i elektroniske kommunikasjonsnett eller -tjenester og datasenter. Dette gjelder data som både er lagret, overført og håndtert, samt tjenester som tilbys gjennom eller gjøres tilgjengelige via slike nett eller tjenester[2]. Forsvarlig sikring er en rettslig standard som skal utvikles over tid i takt med teknologisk utvikling, markedsforhold og samfunnsbehov.

Samfunnssikkerhet handler om evnen til å verne samfunnet mot og håndtere hendelser som truer viktige verdier og funksjoner, eller setter liv og helse i fare. Slike hendelser kan skyldes naturkatastrofer, tekniske eller menneskelige feil, eller være resultat av bevisste handlinger[3]. I hovedinstruksen for Nkom fremgår det at Nkom har en rolle og et ansvar i samfunnssikkerhetsarbeidet.

Grunnleggende nasjonale funksjoner (GNF) er tjenester, produksjon og annen virksomhet som er så viktige at et helt eller delvis bortfall vil påvirke statens evne til å verne nasjonale sikkerhetsinteresser[4].

Risiko handler alltid om fremtidige hendelser og den usikkerheten som følger med dem. Usikkerheten gjelder både om en bestemt, uønsket hendelse vil oppstå og hvilke konsekvenser den kan få. Man forstår dermed risiko som mulige uønskede hendelser og de konsekvensene som følger etter.

Sårbarhet er et uttrykk for de problemene et system vil få med å fungere når det utsettes for en uønsket hendelse, og de problemene systemet får med å gjenoppta sin funksjon etter at hendelsen har inntruffet. Sårbarheten til systemet kan påvirke både sannsynligheten for og konsekvensene av en hendelse[5].

Et system eller ekomnett er satt sammen av ulike nettverkslag[6] og nettelementer. Den fysiske infrastrukturen, som fiberkabler, forsterkere og annet utstyr som bærer de elektromagnetiske signalene, ligger nederst. På nettverks- og transportlagene settes IP-nett og ruting opp. Øverst, på applikasjonslaget, realiseres kommunikasjonstjenester ut til brukerne. Avhengig av systemet kan dette også inkludere organisatoriske faktorer, som for eksempel personell, rutiner og prosedyrer.

Kritisk infrastruktur er anlegg og systemer som er nødvendige for å videreføre eller gjenopprette samfunnets kritiske funksjoner.

Usikkerhet kan uttrykkes på ulike måter, ofte gjennom beregning av sannsynlighet, men slike beregninger alene gir ikke et fullstendig bilde. Risiko handler om fremtiden – noe som kan skje, men som vi ikke kan være helt sikre på når, hvordan eller med hvilke konsekvenser. Altså er fremtiden prinsipielt usikker, og usikkerhet er igjen et vesentlig element i begrepet risiko. Usikkerhet kan deles inn i tre hovedkategorier:

- Fortid: Knyttet til kvaliteten på observasjoner og informasjon Nkom har, samt hvordan denne er tolket og forstått.
- Nåtid: Gjelder Nkoms nåværende oversikt relatert til ekomnett, tjenester, kritisk infrastruktur, aktører og forståelsen av trusselbildet, samt sammenhengen mellom disse.
- Fremtid: Fremtiden er grunnleggende usikker, og denne usikkerheten kan ikke reduseres.


Foto: Nkom

Beredskap er planlagte og forebyggende tiltak som gjør en aktør i stand til å håndtere uønskede hendelser slik at konsekvensene blir minst mulig, med mål om at normaltilstanden raskt kan gjenopprettes. Beredskap skal sørge for at man kan håndtere risiko som ikke kan forebygges[7].

Ekomloven skal bidra til å styrke sikkerhet og forbrukernes rettigheter innen elektronisk kommunikasjon. Loven stiller krav til forsvarlig sikring i den digitale infrastrukturen og gir Nkom viktige verktøy for å sikre at brukerne har tilgang til gode, sikre og fremtidsrettede tjenester. Den nye ekomloven trådte i kraft 1. januar 2025 og viderefører reguleringen av mobil- og bredbåndstjenester, internettbaserte applikasjoner og sosiale medier, og omfatter for første gang spesifikk regulering av datasentre, inkludert krav til registrering, sikkerhetsstyring og beredskapsrutiner[8].

Sikkerhetsloven skal bidra til å forebygge, avdekke og motvirke virksomhet som truer sikkerheten, samt tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. Nkom har ansvaret for å føre tilsyn med tilbyderne

som er underlagt sikkerhetsloven innenfor datasentre og ekomsektoren. Sikkerhetsloven bygger på sektorprinsippet, som innebærer at ulike departementer kan fatte vedtak om hvilke virksomheter innenfor sitt ansvarsområde som skal omfattes av sikkerhetsloven. Det finnes ingen offentlig oversikt over hvilke selskaper i Norge som er underlagt regelverket[9].

Lov om elektroniske tillitstjenester gjennomfører eIDAS-forordningen[10] i norsk rett og etablerer blant annet selvdeklarasjonsordninger og tilsyn. eIDAS er et felles europeisk rammeverk for elektronisk identifikasjon (eID) og kvalifiserte tillitstjenester, med formål om å sikre tillit, interoperabilitet og sikker digital samhandling på tvers av landegrensene i EU[11]. I Norge er Nkom utpekt som tilsynsmyndighet og kontrollerer om tilbyderen oppfyller kravene i loven og eIDAS. Det er besluttet og innført en endringsforordning i EU omtalt som eIDAS2 som endrer eIDAS-forordningen.

[2] https://lovdata.no/dokument/NL/lov/2024-12-13-76/KAPITTEL_3#KAPITTEL_3
[3] https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/
[4] https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker/veileder-i-departementenes-identifisering-av-grunnleggende-nasjonale-funksjoner/grunnleggende-nasjonale-funksjoner/
[5] https://www.dsb.no/ros-og-beredskap/statsforvalteren/fylkesros/
[6] 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.)
[7] https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker/veileder-i-departementenes-identifisering-av-grunnleggende-nasjonale-funksjoner/grunnleggende-nasjonale-funksjoner/
[8] https://nkom.no/aktuelt/stortinget-har-behandlet-ny-ekomlov
[9] https://nkom.no/sikkerhet-og-beredskap/tilbyders-sikkerhets-og-beredskapsplikter
[10] (EU) nr. 910/2014
[11] eIDAS-forordningen om elektroniske transaksjoner i det indre marked basert på eID og e-signatur | europalov

Foto: Nkom





Foto: Nkom

2 FARER, TRUSLER OG SÅRBARHETER I SEKTOREN

Ekomsektoren utgjør en sentral del av samfunnets kritiske infrastruktur og må derfor beskyttes mot et bredt spekter av farer, trusler og sårbarheter. Dette kapittelet beskriver de viktigste utfordringene knyttet til sikkerhet og robusthet i sektoren, samt forslag til risikoreduserende tiltak. Kapittelet omfatter både tilsiktede handlinger, som cyberangrep og svindel, og utilsiktede hendelser, som naturhendelser og feil i forbindelse med planlagt arbeid.

Videre belyses sårbarheter i verdi- og leverandørkjeder som kan påvirke tilgjengeligheten og integriteten til kritiske tjenester. Det rettes også oppmerksomhet mot satellittbaserte tjenester, som er grunnleggende for mange ekomfunksjoner, og som i økende grad er utsatt for forstyrrelser og manipulering.

Nkom har etablert et kunnskapsgrunnlag om årsaker til utfall i sektoren basert på regionale analyser, innrapporterte hendelser, oppfølging av hendelser og gjennomførte tilsyn. Internasjonalt samarbeid og samarbeid med andre offentlige virksomheter inngår også i grunnlaget for vurderingene av risikobildet.

2.1 STATLIGE TRUSLER

Den sikkerhetspolitiske utviklingen bidrar til økt risiko for ekomsektoren, særlig knyttet til etterretningsvirksomhet og uautorisert tilgang til kritiske systemer. Vurderingene av statlige trusler i dette kapittelet bygger på de åpne nasjonale trussel- og risikovurderingene for 2025 fra Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten. Samlet gir disse vurderingene et situasjonsbilde av utviklingen i det nasjonale og internasjonale trussellandskapet, og danner grunnlaget for beskrivelsen av statlige trusler mot ekomsektoren.



Etterretningstjenesten vurderer at den sikkerhetspolitiske situasjonen er mer spent nå enn ved inngangen til 2025[12]. PST understøtter dette bildet og fremhever at Norge befinner seg i den mest alvorlige sikkerhetspolitiske situasjonen siden andre verdenskrig[13]. Samtidig peker de hemmelige tjenestene på Russland som den største trusselen mot Norge. Både PST og Etterretningstjenesten understreker imidlertid viktigheten av å unngå selvskremming, og fremhever behovet for en kunnskapsbasert tilnærming, der evnen til å skille reelle trusler fra støy, er sentralt.

PST vurderer at russiske aktører kartlegger kritisk infrastruktur i Norge, med sikte på at informasjonen senere kan benyttes til sabotasje eller påvirkningsoperasjoner i en tilspisset konfliktsituasjon. Parallelt forventes det at Kina vil drive omfattende informasjonsinnhenting og kartlegging av norsk digital infrastruktur, primært for etterretningsformål.

Videre har situasjonen i Midtøsten eskalert som følge av amerikanske og israelske angrep mot Iran. PST vurderer situasjonen som uforutsigbar, med en rekke usikkerhetsmomenter. Terrortrusselnivået i Norge er imidlertid uendret og vurderes fortsatt som moderat[14]. Samtidig forventer PST at iranske sikkerhets- og etterretningstjenester vil gjennomføre etterretnings- og påvirkningsoperasjoner i Norge i løpet av året, hvor bruk av proxyaktører fremheves som en sannsynlig fremgangsmåte.

2.1.1 Cyberdomenet

Cyberoperasjoner rammer bredt og utgjør en sentral del av det samlede trusselbildet[15]. Dette gjelder særlig statlige aktører i cyberdomenet, hvor den kinesiske trusselen vurderes som fremtredende[16]. Samtidig peker internasjonale vurderinger på et høyt nivå av cyberkriminalitet og cyberspionasje[17], noe som samlet understreker behovet for høy digital motstandsdyktighet.

2.1.2 Fysisk sabotasje

Antallet fysiske sabotasjeaksjoner i Europa som knyttes til Russland, gikk noe ned i 2025[18]. Samtidig vurderes det at Russland fortsatt kan ha interesse av å gjennomføre sabotasjeaksjoner mot mål i Norge. Eiendom og logistikkinfrastruktur knyttet til norsk støtte til Ukraina fremstår som de mest sannsynlige målene, men PST advarer om at også sivil infrastruktur kan bli rammet.

Myndigheter og virksomheter bør ta dette på alvor og iverksette forebyggende tiltak for å sikre verdier og redusere sårbarheter. Systematisk arbeid med sikring, etablering av reserveløsninger og god reparasjonsberedskap er viktigere enn noen gang.

Fysisk sabotasje utgjør en reell trussel mot kritisk infrastruktur, og kan gjennomføres ved hjelp av ulike metoder. Internasjonale eksempler på sabotasjeforsøk omfatter digitale angrep mot europeiske jernbaner, fysiske innbrudd i vannkraftverk i Tyskland, Sverige og Finland, angrep mot global flyfrakt og omfattende brannstiftelser, blant annet i Warszawa i Polen. Slike hendelser illustrerer at fysiske angrep kan få store konsekvenser for samfunnskritiske funksjoner og tilgjengelighet til tjenester.

2.1.3 Personellsikkerhet og innsidertrusler

Personell utgjør en sentral del av virksomheters sikkerhetsgrunnlag, men representerer også en betydelig risiko. NSM understreker i Risiko 2026 at tekniske sikkerhetstiltak alene ikke er tilstrekkelige dersom virksomheter ikke har kontroll på personellsikkerheten. Som påpekt av NSM under pressekonferansen i forbindelse med lanseringen av Risiko-rapporten den 6. februar 2026:

> *“Det hjelper lite med god digital sikkerhet hvis man har en innsider.*



Foto: Nkom

> *“Tilbydere av samfunnskritiske nett og tjenester, samt colocation-datasenteroperatører, fremstår som særlig attraktive mål for etterretning og innsidevirksomhet.*

God personellsikkerhet forutsetter derfor tydelig ledelse, en sterk sikkerhetskultur og kontinuerlig oppfølging. Klarering og autorisering er viktige mekanismer, men gir kun et øyeblikksbilde av risikoen.

PST[19] advarer om at personer med tilknytning til autoritære stater kan være særlig utsatt for press eller påvirkning, noe som åpner for et bredere spekter av virkemidler fra trusselaktører. Innsidere kan forårsake betydelig skade ettersom de, i kraft av sin rolle, ofte har legitim tilgang til systemer og kan operere innenfor etablerte sikkerhetsmekanismer.

Aktuelle hendelser illustrerer hvordan innsiderrisiko også kan ta form gjennom mer skjulte metoder. Det er blant annet avdekket tilfeller der nordkoreanske IT-aktører infiltrerer virksomheter ved bruk av falske identiteter, blant annet gjennom rekrutteringsplattformer som LinkedIn[20].

Slike aktører kan både bidra til finansiering av regimet og oppnå tilgang til virksomheters systemer, med potensial for uttrekk av teknologi og sensitiv informasjon.

Tilbydere av samfunnskritiske nett og tjenester, samt colocation-datasenteroperatører, fremstår som særlig attraktive mål for etterretning og innsidevirksomhet. Kartlegging av virksomheter kan benyttes til å identifisere sårbarheter og angrepsflater i infrastruktur og tjenester, som senere kan utnyttes i en tilspisset sikkerhetspolitisk situasjon.

2.1.4 Vurderinger og risikoreduserende tiltak

Nkom vurderer at trusselbildet mot sektoren må forstås helhetlig på tvers av cyberdomenet, fysisk sabotasje og innsiderrisiko. Selv om ulike trusseltyper har ulike inngangsvektorer, vil konsekvensene ofte kunne ramme den samme underliggende infrastrukturen.

Nkom har per i dag ikke informasjon som indikerer økt risiko for fysisk sabotasje rettet mot sektoren i 2026. Lokale skader på fysiske enkeltkomponenter, som basestasjoner, vurderes i utgangspunktet å ha begrensede konsekvenser

> *Nkom vurderer cyberoperasjoner med mål om skjult tilgang til digital infrastruktur som en av de mest kritiske truslene mot sektoren.*

utover lokal dekning, som ofte er overlappende. Samtidig kan ekominfrastruktur være samlokalisert med annen infrastruktur som i større grad kan være mål for sabotasje. Hendelser rettet mot slike mål kan gi spillovereffekter og indirekte ramme ekomtjenester.

Nkom fremhever videre konsentrasjonsrisiko som en sentral sårbarhet i sektoren. Høy grad av avhengighet til enkeltleverandører eller enkeltlokasjoner kan redusere robustheten i tjenesteleveransen. Et sentralt tiltak er derfor å spre kritiske funksjoner og ressurser på flere leverandører og løsninger. Systematisk sikringsarbeid, etablering av reserveløsninger, redundans og god reparasjonsberedskap er avgjørende for å styrke robustheten og redusere konsekvensene ved bortfall av kritiske knutepunkter.

Erfaringer fra ekstremværshendelser i Norge viser at ekominfrastruktur kan bli utilgjengelig over større områder og over tid, særlig som følge av kraftutfall kombinert med fiberbrudd og/eller transmisjonsbrudd. For å oppnå tilsvarende eller større effekt gjennom tilsiktede handlinger, vurderes det at en statlig aktør trolig vil benytte cyberdomenet som inngangsvektor. Nkom vurderer cyberoperasjoner med mål om skjult tilgang til digital infrastruktur som en av de mest kritiske truslene mot sektoren. Slik tilgang kan oppnås gjennom flere metoder, herunder fjernaksess, kontokompromittering, brute force-angrep, innsidere, nulldagssårbarheter og bruk av skjult utstyr.

NSM anbefaler at virksomheter benytter cybersjekk.no[21] for å få oversikt over egen cybersikkerhet, og som et grunnlag for å styrke beskyttelsen mot både digital kriminalitet og statlige cyberoperasjoner.

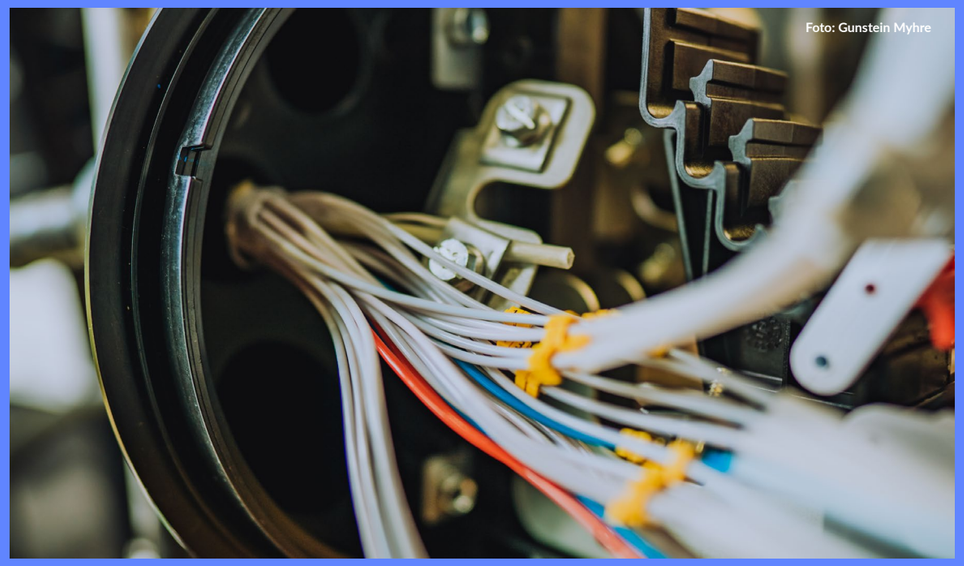
Følgende risikoreduserendetiltak retter seg primært mot relevante myndigheter, virksomheter med samfunnssikkerhetsansvar, samt tilbydere av ekomnett- og tjenester:

---

[12] Fokus 2026 - Etterretningstjenesten
[13] https://www.pst.no/sjef-pst-i-ntv-2026-vi-beskriver-et-alvorlig-trusselbilde/
[14] Nasjonal trusselvurdering 2026 - pst.no
[15] Risiko 2026 - Nasjonal sikkerhetsmyndighet
[16] Nasjonal trusselvurdering 2026 - pst.no
[17] https://mssb.dk/nyheder/nyhedsarkiv/2025/november/cybertruslen-mod-danmark-er-alvorlig/
[18] Risiko 2026 - Nasjonal sikkerhetsmyndighet
[19] Nasjonal trusselvurdering 2026 - pst.no
[20] PST: Nord-Korea bruker falske identitetar for å spionere på norske bedrifter – NRK Norge – Oversikt over nyheter fra ulike deler av landet
[21] Cybersjekk

Risikoreduserende TILTAK

- Gjennomgå og eventuelt oppdatere planer for beskyttelse av egen infrastruktur.
- Kontrollere og kvalitetssikre planer for risikoreduserende tiltak.
- Sikre at alle ansatte har tilstrekkelig risiko- og sikkerhetsforståelse i lys av dagens sikkerhetspolitiske situasjon.
- Benytte NSMs cybersjekk.no for å kartlegge og styrke egen cybersikkerhet.
- Ha fokus på sikkerhetsstyring i alle ledd, herunder:
  - Etablere og opprettholde oversikt over verdier og avhengigheter.
  - Etablere eller oppdatere rutiner for oppdatering av programvare.
  - Begrensning av tilgang og aksess til systemer og informasjon.
- Utøve god sikkerhetsledelse, inkludert kjennskap til egne ansatte.
- Vurdere bruk av sikkerhetstesting, eksempelvis målrettet testing for å avdekke sårbarheter i systemer og tjenester.
- Etablere og vedlikeholde beredskapsplaner for redundans, reserveløsninger og reparasjon etter hendelser.


Foto: Gunstein Myhre

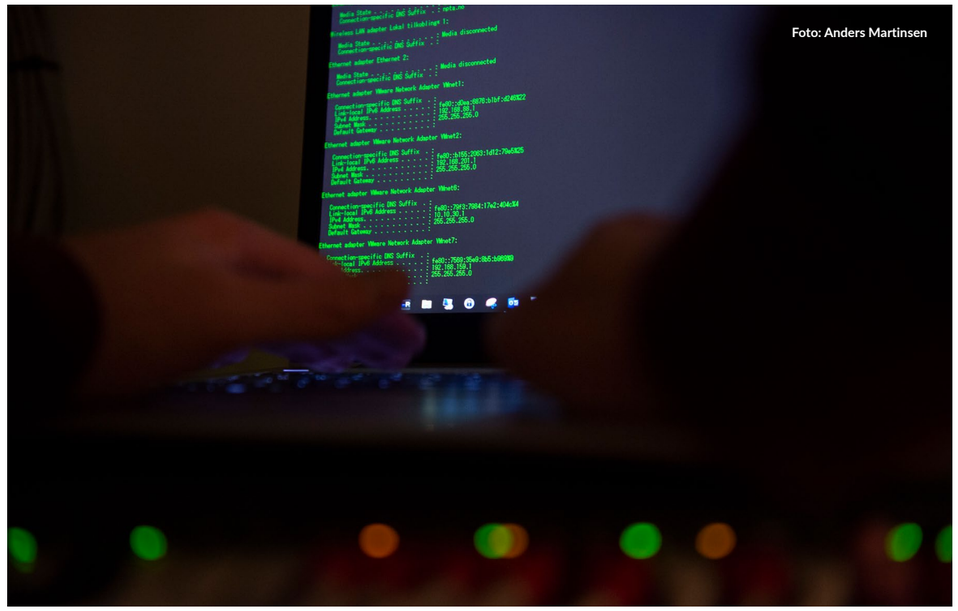


Foto: Anders Martinsen

2.2 SÅRBARHETER I CYBERDOMENET

Ekomtilbydernes evne til å motstå cyberangrep og opprettholde kontinuitet er avgjørende for stabiliteten i moderne ekomnett. Cyberangrep kan påvirke både system- og databeskyttelse. Angrepene spenner fra støyende og kapasitetskrevende hendelser til skjulte og langvarige operasjoner rettet mot kritisk infrastruktur. Generelt er det enklere å oppdage og motvirke synlige hendelser, som tjenestenektangrep (DDoS-angrep) og større driftsavvik, enn avanserte, skjulte og vedvarende angrep, som ofte er vanskeligere og mer ressurskrevende å avdekke.

Trusselbildet i cyberdomenet

Internett-ruting er basert på Border Gateway Protocol (BGP[22]), en tillitsbasert protokoll uten innebygde mekanismer for verifisering av ruteopprinnelse eller relasjoner mellom nettverksoperatører. Dette gjør infrastrukturen sårbar for feilkonfigurasjoner, rutelekkasjer og bevisste kapringer, med mulige konsekvenser som trafikkavbrudd, feilruting og i enkelte tilfeller avlytting eller manipulering av trafikk. Sikkerhetsmekanismer som skal redusere denne risikoen, er under stadig utvikling og krever tett oppfølgning hos alle ekomaktører.

Datainnbrudd og løsepengevirus har økt i omfang og kompleksitet og utgjør en vedvarende trussel også mot ekomsektoren. Risikoen for at slike angrep påvirker tjenesteproduksjonen hos ekomaktører, forsterker konsekvensene i ekomsektoren. I løpet av 2025 og 2026 er det rapportert om vellykkede angrep mot blant annet Telia:

Datainnbrudd hos Telia Norge

Den 16. februar 2026 melder NRK at Telia Norge hadde blitt utsatt for et omfattende datainnbrudd, der store mengder data var gjort tilgjengelig på det mørke nettet.

Ifølge Telia ble innbruddet oppdaget i slutten av november 2025 i en avgrenset del av selskapets IT-miljø. Trusselaktøren skal ha hatt tilgang til Telias nettverk over en lengre periode, og over 400 000 filer, tilsvarende om lag 2,5 TB data, ble gjort tilgjengelig på det mørke nettet.

NRK opplyste at materialet omfattet flere tusen bilder, over 10 000 regneark og mer enn 20 000 PDF-filer. Det ble også rapportert om store mengder metadata knyttet til telefonikunder som var kommet på avveie. De nyeste filene skal ha vært fra september 2025.

Bergen kommune opplyste i en pressemelding at kommunen var blant de berørte virksomhetene. Mellom 2 000 og 2 500 ansatte og politikere i Bergen kommune skal ha fått navn, telefonnummer samt telefon- og SMS-logger eksponert. Det ble samtidig presisert at innholdet i meldingene ikke var tilgjengelig. Foreløpige vurderinger indikerte at opplysningene omfattet perioden fra 2021 til april 2025.

Det ble videre rapportert at 17 norske kommuner var berørt av hendelsen, og at saken var under politietterforskning.

Den 12. mars 2026 opplyste Kripos at de hadde identifisert aktøren bak angrepet og avdekket hvordan innbruddet skal ha skjedd.

> *“Datainnbrudd og løsepengevirus har økt i omfang og kompleksitet og utgjør en vedvarende trussel også mot ekomsektoren.*

Løsepengevirus, verdikjedeangrep og statsstøttet spionasje bidrar samlet til et mer komplekst trusselbilde, hvor aktører i økende grad søker vedvarende og skjult tilgang til kjernenett, nettverkskomponenter og sensitiv informasjon. Økende kompleksitet i systemlandskapet, økt leverandøravhengighet og utstrakt bruk av automatiserte og KI-baserte driftsløsninger gjør kontroll, etterprøvbarhet og hendelseshåndtering mer krevende.

Kunstig intelligens får samtidig økende betydning både som mulighet og som trussel i ekomsektoren. Bruken av KI i nettverksproduksjon og konfigurasjon

øker, og inngår i stadig større grad i overvåkning, feilanalyse og optimalisering av ekomtjenester.

Formålet er effektivisering, økt robusthet, bedre utnyttelse av nettressurser og raskere respons ved feil og hendelser. KI kan dermed bidra til å styrke sikkerhet, drift og beredskap i sektoren. Bruk av KI kan også gi særskilte sårbarheter fordi det ofte er vanskelig å se hvordan modellen kommer fram til et svar eller i verste fall brukes til en ondsinnet handling. Hvis modellen gir feil eller uventede resultater, kan det derfor være krevende å finne ut hvorfor. Dette omtales gjerne som «svart boks»-problematikk. Videre kan økt bruk av KI føre til sterkere avhengighet av leverandører, proprietære modeller og sky-tjenester, noe som kan redusere operatørenes kontroll over funksjonalitet, endringshåndtering og bruk av driftsdata. Utbredt bruk av de samme komponentene kan også gi felles sårbarheter på tvers av sektoren, der feil eller kompromittering hos én aktør kan få konsekvenser for store deler av sektoren samtidig.

Utviklingen av stadig større og mer avanserte KI-modeller (frontier-modeller), herunder systemer med evne til selvstendig planlegging, verktøybruk og gjennomføring av komplekse oppgaver, bidrar til en rask endring av risikobildet innen programvare- og kodesikkerhet. Dette gjelder særlig programvare som inngår i produksjon og leveranse av elektroniske kommunikasjonstjenester, hvor sikkerhetshendelser kan få betydelige konsekvenser for konfidensialitet, integritet, tilgjengelighet og stabilitet i mobil- og ekomnett. Kompetansebarrierene for ondsinnede aktører kan reduseres, samtidig som tempoet i identifisering og utnyttelse av sårbarheter øker. På kort sikt kan dette føre til mer omfattende utnyttelse av nulldagssårbarheter og et mer uforutsigbart trusselbilde. På lengre sikt kan de samme kapabilitetene bidra til bedre kodekvalitet og styrket sikkerhet i programvare. Den samlede effekten vil være avhengig av hvordan slike kapabiliteter utvikles, hvilke modeller det gis tilgang til, og hvordan de gjøres tilgjengelige i markedet. Denne utviklingen er allerede synlig hos store programvareleverandører, som tilpasser sårbarhetshåndteringen til økt tempo i identifisering, publisering og oppfølging av sikkerhetsfeil. Dette stiller samtidig økte krav til ekomaktørenes rutiner for testing og oppdatering av egen infrastruktur.

2.2.1 Vurderinger og risikoreduserende tiltak

Trusselbildet i cyberdomenet preges av økende kompleksitet og mer avanserte angrepsmetoder, noe som skjerper kravene til både tekniske og organisatoriske tiltak. Sentrale utfordringer omfatter håndtering av tjenestenektangrep, sikring av ruting i internettinfrastrukturen, samt styrket kontroll med leverandører og tilgang til kritiske systemer.

Effektiv håndtering av volumetriske tjeneste–nektangrep forutsetter distribuert mitigering, automatisert respons og tett samarbeid mellom aktører. KI-baserte løsninger kan bidra til raskere deteksjon av avvik, bedre analyse av trafikkmønstre og mer presis prioritering av tiltak. Samtidig kan økt automatisering gi nye sårbarheter dersom beslutningsgrunnlaget er feil, modellene er manipulerbare, eller responsmekanismene ikke er tilstrekkelig testet og kontrollert.

Mekanismer som BGP blackholing og FlowSpec[23] legger til rette for rask filtrering av trafikk nær kilden. Samtidig medfører slike tiltak økt kompleksitet og risiko for feil, som må håndteres gjennom prosedyrer, testing og operasjonell kontroll.

Risiko knyttet til ruting kan reduseres gjennom økt bruk av kryptografiske mekanismer for verifisering, herunder RPKI[24] for validering av ruteopprinnelse og ASPA for kontroll av

KI-akselerert sårbarhetsfunn hos global nettverksleverandør

I juni 2026 varslet Cisco at kunstig intelligens og automatiserte analyseverktøy gjør det mulig å avdekke sårbarheter i store kodebaser i et langt høyere tempo enn tidligere. Som følge av dette endrer selskapet sin modell for sårbarhetshåndtering, med planlagte sikkerhetspubliseringer to ganger i måneden og forhåndsvarsling til kunder syv dager før publisering. Cisco peker på at tradisjonell, enkeltsaksbasert håndtering av sårbarheter ikke lenger er tilstrekkelig når tiden fra offentliggjøring til mulig utnyttelse blir kortere.

For virksomhetene innebærer utviklingen økte krav til oversikt over egne systemer, leverandøroppfølging, testing og evne til å gjennomføre sikkerhetsoppdateringer innenfor kontrollerte endringsvinduer. Kortere tid mellom publisering av en sårbarhet og mulig utnyttelse reduserer samtidig handlingsrommet for å vurdere, teste og implementere nødvendige tiltak.


Foto: Nkom

relasjoner mellom nettverk. Effekten av tiltakene forutsetter høy implementeringsgrad, korrekt forvaltning av autorisasjonsdata og konsekvent valideringspraksis. Tiltakene bør suppleres med overvåking av ruteannonseringer, styrket tilgangskontroll til administrative systemer og evne til å avdekke unormale mønstre i ruting og trafikkflyt.

For å redusere risiko for løsepengevirus og datainnbrudd er det behov for helhetlige sikkerhetstiltak. Dette omfatter tydelige sikkerhetskrav til leverandører og systematisk oppfølging av disse, kontinuerlig identifisering og håndtering av sårbarheter, samt sterk tilgangskontroll, herunder bruk av multifaktorautentisering og nettverkssegmentering. KI kan understøtte dette arbeidet gjennom mer effektiv sårbarhetsanalyse, prioritering av tiltak og støtte til hendelseshåndtering. Samtidig kan KI-baserte verktøy også senke terskelen for ondsinnede aktører, blant annet gjennom raskere utvikling av skadevare, mer målrettet sosial manipulering og mer effektiv utnyttelse av kjente og ukjente sårbarheter.

Videre bør datamengder begrenses gjennom hensiktsmessige sletterutiner, og det bør etableres robuste, isolerte og regelmessig testede reserveløsninger. Det vil fortsatt foreligge en vedvarende restrisiko, som må håndteres gjennom kontinuerlig forbedring, styrket beredskap og operasjonell kontroll med både teknologiske og organisatoriske sikkerhetstiltak.

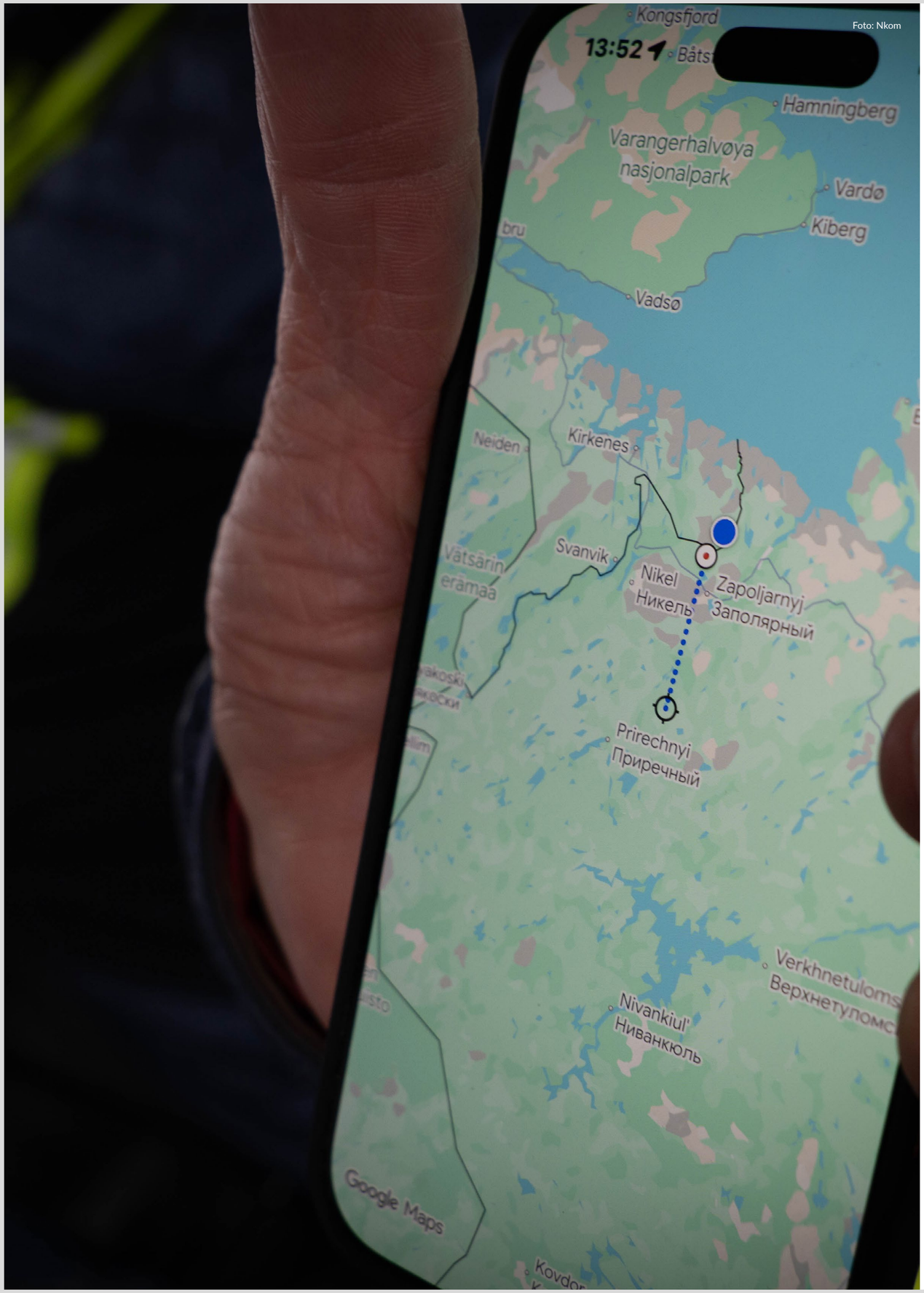
Følgende risikoreduserende tiltak retter seg primært mot relevante myndigheter, virksomheter med samfunnssikkerhetsansvar, samt tilbydere av ekomnett- og tjenester:

[22] BGP er en grunnleggende protokoll som brukes på internett for å rute trafikk mellom ekomaktører
[23] Mekanismer i BGP som brukes for å signalere til andre ekomaktører et behov for å filtrere uønsket trafikk
[24] Påbygg til BGP som lar nettverkseier signalisere eierskap til bestemte IP-adresser og som tillater mottakere av trafikk å filtrere trafikken.

SÅRBARHETER I CYBERDOMENET

Risikoreduserende
TILTAK

- Følge utviklingen og implementere tilstrekkelige løsninger for håndtering av tjenestenekt-angrep.
- Sikre at transittavtaler og samtrafikkpunkt BGP-avtaler inkluderer mekanismer for håndtering av distribuerte tjenestenektangrep.
- Etablere og vedlikeholde mekanismer for sikker ruting.
- Innføre overvåking av egne ruteannonseringer for å avdekke avvik eller uautoriserte annonseringer.
- Stille tydelige sikkerhetskrav til leverandører og begrense deres tilgang til utviklings- og produksjonsmiljøer.
- Etablere rutiner for identifisering og håndtering av sårbarheter, inkludert systematisk oppdatering og overvåking
- Benytte tilgangsstyring, segmentering av nettverk og flerfaktorautentisering for å redusere risikoen for uautorisert tilgang.
- Etablere sikre reserveløsninger og teste gjenoppretting jevnlig.
- Sørge for rask identifikasjon, overvåking og isolering av kompromitterte komponenter og miljøer.
- Forankre ansvar for leverandør- og verdikjederisiko i ledelsen og gjennomføre jevnlige risikovurderinger.
- Benytte avviks- og atferdsbasert deteksjon, samt prinsippet om minste privilegium og overvåking av kritiske systemer.
- Sikre kontrollert og trinnvis innføring av KI-systemer, herunder bruk av pilotering før bred implementering.
- Stille krav til dokumentasjon, logging, forklarbarhet og etterprøvbarhet av KI-systemer og beslutninger.
- Vurdere regulatorisk etter-levelse og behov for alternative løsninger eller utfasing dersom KI-funksjonalitet ikke kan tilfredsstille gjeldende eller kommende krav.
- Utvikle kompetanse om KI i sektoren, med særlig vekt på sikkerhet og risikoforståelse.



2.3 POSISJONSBESTEMMELSE, NAVIGASJON OG TIDSBESTEMMELSE (PNT)

PNT[25]- tjenester er levert via satellitt. Den vanligste tilgangsteknologien er en av GNSS[26] -systemene (amerikanske GPS, europeiske Galileo, russiske Glonass eller kinesiske Beidou). Disse tilbyr PNT over hele kloden til enhver tid, vederlagsfritt. Andre systemer og teknologier for å levere P, N og/eller T via (typisk) lavbanesatellitt finnes også, for eksempel Satelles (som tilbyr tidstjenester) eller Iridium (som tilbyr posisjonsbestemmelse). Andre aktører, som Xona og Thales, utvikler også nye løsninger. Det er forventet at nye teknologier og aktører vil dukke opp for å levere P, N og/eller T via satellitt, i hovedsak fra satellitter i lavbane. Disse tjenestene vil antagelig ikke være vederlagsfrie slik som GNSS-systemene i dag, men ha andre fordeler som eksempelvis mer robuste signaler, autoriseringsmekanismer og redundans. Det er også forventet at de i stor grad vil bli brukt i sammenheng med eksisterende GNSS-systemer og ikke erstatte dem.

Sikkerhetssituasjonen i Norge i dag er sammensatt. Det registreres økende forekomst av GNSS-interferens i det sivile samfunnet med en stigende hendelsestrend over tid (se Figur 4). Samtidig observeres det omfattende og mer intense forstyrrelser i nordlige grenseområder, som tilskrives aktivitet fra Russland. Situasjonsbildet er i hovedsak uendret fra tidligere år. De mest fremtredende utfordringene på landsbasis knytter seg til transport (særlig syketransport), sporingssystemer og anleggsvirksomhet. Samtidig er sivil luftfart betydelig påvirket i luftrommet over Øst-Finnmark som følge av GNSS-forstyrrelser, både i form av jamming (frekvensblokkering) og spoofing (manipulering av posisjonssignaler).

Sammenliknet med tidligere år observeres det at forstyrrelsene i Finnmark nå oppleves i lavere luftlag[27], også nært bakkenivå. Det er videre indikasjoner på at kilder til slike forstyrrelser har fått økt utbredelse og dekning, noe som kan medføre at nye områder i Finnmark over tid kan bli berørt. Dette kan få konsekvenser for tjenester og funksjoner som er avhengige av presis posisjonsbestemmelse og tidsreferanser fra satellitt.

Internasjonalt er GNSS-forstyrrelser et økende problem, særlig for luftfart[28] og maritim sektor[29]. Forstyrrelsene oppstår primært i tilknytning til konfliktområder som Ukraina og Iran, men sprer seg ofte utover disse områdenes geografiske grenser. Dette kommer blant annet til uttrykk i Østersjøen og i Nord-Norge.

Utviklingen henger sammen med en betydelig økning i bruken av små, GNSS-styrte droner de siste årene, særlig etter Russlands fullskala invasjon av Ukraina. Omfattende bruk av slike systemer har for første gang blitt en integrert del av moderne konvensjonell krigføring.



Figur 4 GNSS i det sivile samfunnet og utviklingen i antall hendelser over tid

Menon Economics har gjennomført en samfunns–økonomisk analyse[30] av kostnadene for det norske samfunnet ved et fullstendig bortfall av GNSS i en syvdagersperiode. Analysen estimerer kostnadene til 3,4 milliarder kroner, med sektorene olje og gass, maritim, anlegg og vei som de mest berørte. Hovedpunktene fra deres sårbarhetsanalyser viser at konsekvensene vil øke i takt med videre digitalisering av samfunnet; at PNT utgjør en usynlig, men kritisk, infrastruktur; at flere sektorer er avhengige av presis tid, men at mange har redundans for kort- til mellomlange GNSS-bortfall; samt at tilsiktet signalmanipulasjon (spoofing) kan ha større konsekvenser enn rene signalbortfall.

FFI[31] har i samme periode gjennomført analyser av satellittbasert PNT og dens verdi for totalforsvaret. De peker på trusler som frekvensforstyrrelser, anti-satellittvåpen, romvær, romskrot, skader på bakkestyringsinfrastruktur og cyberangrep. Videre

> *“*
> ***GNSS er særlig kritisk for nødtjenester og krisehåndtering, hvor bortfall vil føre til økt etterspørsel etter begrensede alternative løsninger og økt arbeidsbelastning.***

fremheves at tjenester som GNSS forbedrer samfunnstjenester og styrker totalforsvaret, samtidig som samfunnets avhengighet til GNSS medfører sårbarhet. GNSS er særlig kritisk for nødtjenester og krisehåndtering, hvor bortfall vil føre til økt etterspørsel etter begrensede alternative løsninger og økt arbeidsbelastning. Det påpekes også at videre digitalisering av samfunnet vil medføre et økende behov for presis tid, som i dag ofte leveres via satellitt.

Nkoms egne observasjoner understøtter disse vurderingene fra Menon og FFI, særlig knyttet til digitalisering. Undersøkelser gjennomført under Jammertesten på Andøya viser at det finnes betydelige digitale trusler i mange systemer knyttet til spoofing-baserte tidsangrep. Dette representerer en gråsone der angrep kan gjennomføres uten å bli oppdaget, og hvor tidsinformasjonen er en direkte og ubeskyttet inngangsport til digitale systemer. Slike sårbarheter oppstår ofte fordi GNSS inngår som system-i-system, og fordi PNT-informasjonen fra dem i stor grad forblir usynlig, slik Menon påpeker. Angrepsvektorer som spoofing og jamming mot PNT, gjennom blokkering eller manipulasjon av GNSS-signaler, utgjør derfor en økende trussel i takt med økt bruk av GNSS, og det finnes mange mulige angrepsvektorer og forsvarssvakheter.

Samtidig finnes det utviklingstrekk som i noen grad reduserer disse sårbarhetene. Dette inkluderer økt bevisstgjøring om truslene mot GNSS, blant annet som følge av krigen i Ukraina. Videre er nullstyringsantenner (Controlled Reception Pattern Antenna, CRPA) fjernet fra USAs liste over regulert militært utstyr[32] og dermed kan tas i bruk i større grad i det sivile samfunnet.

Autoriseringsmekanismer, som det eksisterende OSNMA[33]-signalet fra Galileo eller det kommende Chimera-signalet fra GPS, integreres i økende grad i moderne GNSS-mottakere og gjør spoofing lettere å oppdage. I tillegg bidrar øvelser som Jammertesten til kartlegging og publisering av sårbarheter og mulige tiltak.

2.3.1 Satellittkommunikasjon

I tillegg til PNT benyttes satellitter i økende grad til kommunikasjon. De siste årene har særlig fremveksten av lavbanesystemer (LEO) gitt økt kapasitet og nye tjenester, herunder bredbånd med lav forsinkelse. Dette bidrar til å styrke tilgjengeligheten til elektronisk kommunikasjon, særlig i områder uten mobildekning, som til havs, i fjellet og i nordområdene.

Flere kommersielle aktører tilbyr slike tjenester, blant annet Starlink og OneWeb. Samtidig arbeides det med europeiske løsninger gjennom IRIS, hvor Norge deltar. Dette samarbeidet knytter Norge tettere til europeisk romsamarbeid[34]. I tillegg utvikles nasjonal kapasitet, blant annet gjennom Space Norway.

Det er sårbarheter knyttet til avhengighet av kommersielle aktører utenfor nasjonal jurisdiksjon. For eksempel har krigen i Ukraina vist hvordan den amerikanskeide satellittjenesten Starlink ble tatt i bruk for å opprettholde kommunikasjon etter angrep på telekom- og kraftinfrastruktur. Avhengighet av aktører utenfor nasjonal eller regional kontroll for levering av kritiske kommunikasjonstjenester kan medføre at Norge påvirkes av beslutninger og prioriteringer landet selv ikke har innflytelse over. Samtidig utgjør satellittkommunikasjon et viktig supplement til bakkenett og bidrar til økt robusthet i ekom-infrastrukturen. I Norge er bruk av satellittutstyr i stor grad harmonisert med europeisk regelverk, og mange tjenester kan benyttes uten individuell frekvenstillatelse. Dette gjelder for eksempel brukerutstyr for satellittelefon[35]. Satellittelefoner har global dekning, og gir tilgang til kommunikasjon via satellitter både over vann og på land.

2.3.2 Vurderinger og risikoreduserende tiltak

Distribusjon av robust og presis tid er avgjørende for videre utvikling innen blant annet mobilkommunikasjon, kraftsektoren, datasentre samt nød- og beredskapskommunikasjon. I nasjonal sikkerhetsplan for digital infrastruktur vil regjeringen vurdere etablering av en nasjonal tjeneste for distribusjon av nøyaktig tid som et supplement og en redundans til GNSS.

Det er også behov for å utvide forståelsen av logiske forsvarstiltak til å omfatte hendelser som tidsspoofing, som kan ha konsekvenser tilsvarende tradisjonelle cyberangrep.

Satellitt er fortsatt en teknologiplattform i betydelig utvikling, med stadig nye bruksområder og et økende antall brukere. Samtidig er satellittsystemer sårbare for ulike typer forstyrrelser som kan svekke eller blokkere signalene, blant annet fordi signalstyrken er vesentlig lavere enn for bakkebaserte sendere.

Andre trusler, som romvær og romskrot, bidrar også til økt sårbarhet sammenlignet med bakkebaserte tjenester. Til tross for dette benyttes satellitt i stor utstrekning, ettersom plattformen er svært nyttig for radiokommunikasjon. Nkom vurderer derfor at både videreføring og utvikling av satellittjenester vil fortsette, og at bruken vil øke, særlig innen satellittkommunikasjon, men også satellittnavigasjon.

Følgende risikoreduserende tiltak retter seg primært mot virksomheter med kritiske avhengigheter til PNT og relevante myndigheter:

---

[25] PNT – Posisjonsbestemmelse, Navigasjon og Tidsbestemmelse
[26] GNSS – globalt satellittnavigasjonssystem
[27] https://nkom.no/aktuelt/har-avdekket-nye-alvorlige-gps-forstyrrelser-i-ost-finnmark
[28] https://ops.group/blog/gps-spoofing-final-report/
[29] https://windward.ai/blog/gps-jamming-disrupts-1100-ships-in-the-middle-east-gulf/
[30] Menon-rapport
[31] FFI-rapporten
[32] https://insidegnss.com/crpas-to-be-removed-from-itar-list-opening-market-for-u-s-manufacturers/
[33] OSNMA - Open Service Navigation Message Authentication
[34] http://regjeringen.no/no/aktuelt/norge-og-eu-styrker-samarbeidet-om-sikker-satellittkommunikasjon-med-signering-av-secure-connectivity-avtalen.-na-bindes-norge-tettere-til-europeisk-romsamarbeid/id3154797/?utm_source=regjeringen.no&utm_medium=rss
[35] https://nkom.no/frekvenser-og-elektronisk-utstyr/satellitt/satellittkommunikasjon

POSISJONSBESTEMMELSE, NAVIGASJON OG TIDSBESTEMMELSE (PNT)

Risikoreduserende TILTAK

- Delta i øvelser som Jammertest for å teste og avdekke sårbarheter i systemer som benytter GNSS og PNT.
- Sikre tilstrekkelig redundans i kilder til PNT-informasjon, slik at bortfall i ett system ikke medfører omfattende utfall eller forstyrrelser.
- Isolere PNT-kilder fra hverandre, både fysisk og implementeringsmessig, for å hindre at feil i én kilde påvirker andre.
- Følge utviklingen innen multi-PNT og alternative PNT-løsninger (APNT), og vurdere implementering der det er hensiktsmessig.
- Benytte flere uavhengige GNSS-systemer, herunder europeiske løsninger som Galileo, for å oppnå økt robusthet.
- Utøve god bestillerkompetanse ved anskaffelser for å sikre redundans og utfordre leverandørers forutsetninger og påstander.
- Gjennomføre verdikjede-vurderinger for å identifisere sårbarheter knyttet til teknologi, avhengigheter og forsvarsmekanismer.
- Utvide sikkerhetstiltak til å omfatte både cyberangrep og hendelser som spoofing, som kan ha tilsvarende konsekvenser.



Foto: Nkom

2.4 DIGITAL SVINDEL

Digital svindel er et samfunnsproblem som forekommer på de fleste digitale kanaler og plattformer, og som daglig rammer både privatpersoner og virksomheter. Tall fra Finanstilsynet viser at det økonomiske tapet som følge av svindel i 2024 var på over 1,2 milliarder kroner. Fra andre halvår 2024 til første halvår 2025 ble det imidlertid registrert en reduksjon på 35 prosent i svindlet beløp, fra 616 millioner til 404 millioner kroner[36]. Mobilnetteierne har de siste årene gjennomført flere tiltak for å redusere omfanget av svindel via tale- og SMS-kanalene, noe som kan bidra til å forklare deler av nedgangen. Beløpene er likevel fremdeles høye, og svindelaktørene utvikler stadig nye metoder. De økonomiske tapene bidrar samtidig til å finansiere internasjonal kriminalitet. Oppklaringsprosenten er fortsatt lav.

Undersøkelser gjennomført av Respons Analyse på oppdrag fra Nkom viser en nedgang i tradisjonell telefonsvindel. Seks av ti nordmenn oppga at de hadde blitt utsatt for svindelforsøk over telefon i 2024, mot fire av ti i 2025[37]. Tilsvarende gikk andelen som oppga å ha blitt utsatt for svindelforsøk via SMS ned fra syv av ti i 2024 til fem av ti i 2025.

Norske nummerressurser har på grunn av ulike tiltak blitt vanskeligere å spoofe eller manipulere. Svindlerne må derfor i større grad benytte utenlandske telefonnumre og/eller andre kanaler og metoder, herunder bruk av internettbaserte tjenester og plattformer.

2.4.1 KI som driver for mer sofistikert svindel

Digital svindel skjer i økende grad gjennom et bredt spekter av internettbaserte kanaler og plattformer, herunder e-post, sosiale medier, nettbutikker samt ulike tale- og meldingstjenester. Bruk av kunstig intelligens (KI) har gjort enkelte svindelmetoder mer sofistikerte og troverdige, blant annet gjennom deepfake-teknologi, målrettet genering av feilfrie tekster og utnyttelse av informasjon fra sosiale medier. Samtidig er en stor andel av svindelforsøkene fortsatt basert på tradisjonell sosial manipulasjon uten bruk av kunstig intelligens.

Det foreligger også flere strukturelle sårbarheter. Utfordringer knyttet til tilbakesporing (traceback) gjør det krevende å identifisere aktørkjeder og opprinnelsen til svindelforsøk. Videre kan tilgjengelighet og spredning av abonnentdata og informasjon fra sosiale medier utnyttes i målrettet svindel, for eksempel ved å identifisere grupper som er særlig sårbare for relasjonsbasert svindel. Bruk av kunstig intelligens kan forsterke disse sårbarhetene ved å muliggjøre mer effektiv innsamling, analyse og utnyttelse av slike data i stor skala. Dette kan gjøre svindelmetodene mer presise, målrettede og troverdige. Det er også en sårbarhet at land har ulike regulatoriske og tekniske tiltak for å forebygge og bekjempe digital svindel.

2.4.2 Sårbarheter tilknyttet eID og tillitstjenester

Nkom er per i dag ikke kjent med tilfeller av svindel som direkte skyldes tekniske svakheter i løsningene. De fleste tilfeller av misbruk skjer i nære relasjoner, der personer med tillit, som familie eller bekjente, får tilgang til andres BankID, eller annen eID, for å bistå med praktiske oppgaver. Dette understreker viktigheten av at alle ledd i utstedelse, forvaltning og bruk av eID skjer i henhold til gjeldende sikkerhetskrav og etablerte kontrollmekanismer.

Den reviderte eIDAS-forordningen[38] innebærer en utvidelse av rammeverket, blant annet gjennom etableringen av en europeisk digital identitetslommebok (EUDI Wallet) og nye tillitstjenester. Denne utviklingen legger til rette for økt bruk av digitale identiteter, men medfører samtidig økt kompleksitet og nye sårbarheter. Økt utbredelse og verdi av eID-løsninger kan gjøre dem til attraktive mål for svindel og misbruk, særlig dersom tilliten til løsningene utnyttes. Dette stiller skjerpede krav til sikker implementering, høy tilgjengelighet og oppetid, robust identitetsforvaltning og økt brukerbevissthet. Bortfall av eID kan få betydelige konsekvenser, ettersom en rekke tjenester er avhengige av eID for autentisering og tilgangsstyring. Dette gjelder blant annet innlogging til offentlige tjenester, digitale lommebøker, nettbank og helsetjenester, samt bruk av tillitstjenester som elektronisk signering.

2.4.3 Vurderinger og risikoreduserende tiltak

Nkom arbeider aktivt og langs flere akser for å sikre en trygg og tilgjengelig digital hverdag for alle. Dette gjøres blant annet gjennom å føre tilsyn med etterlevelse av plikten til å blokkere svindel[39] og krav til entydig identifisering[40]. Nkom fører også statistikk over blokkeringstall, leder nasjonale og internasjonale arbeidsgrupper og driver et aktivt informasjonsarbeid.

Digital svindel og svindelforsøk forekommer kontinuerlig, med et bredt spekter av metoder på tvers av de fleste digitale kanaler og tjenester. Nkom vurderer at det ikke er realistisk å eliminere slik aktivitet fullstendig. KI er allerede tatt i bruk i svindelforsøk, og det er grunn til å forvente at omfanget og kompleksiteten vil øke i årene som kommer.

> *“Nkom arbeider aktivt og langs flere akser for å sikre en trygg og tilgjengelig digital hverdag for alle.*

Misbruk av telefonnumre i svindelforsøk

I flere saker det siste året har kunder blitt oppringt av svindlere som utgir seg for å representere politiet eller banker. Svindlerne fremstår ofte profesjonelle og oppgir navn, tjenestenummer og saksnummer for å skape tillit. De kan hevde at kunden er utsatt for et svindelforsøk, eller at noen forsøker å ta opp lån i kundens navn, og oppfordrer deretter kunden til raskt å overføre penger til en såkalt «sikker konto». Det finnes eksempler på at kunder har blitt svindlet for beløp på opptil 100 000 kroner gjennom denne typen svindel.

I eksempler som Nkom har mottatt fra banker, er det observert spoofing av både danske, svenske og nederlandske telefonnumre i ulike typer svindelforsøk.

FNs kontor for narkotika og kriminalitet (UNODC) og Interpol arrangerte 16.-17. Mars Global Fraud Summit[41], der det blant annet ble etablert et rammeverk for offentlig-privat samarbeid mot svindel. Dette kan danne grunnlag for økt internasjonalt samarbeid og større oppmerksomhet på feltet. Det er også foreslått egen bestemmelse om antisvindel i den kommende Digital Networks Act. Dette kan på sikt bidra til økt bevissthet og mer harmoniserte tiltak blant europeiske regulatører.

Når det gjelder eID og tillitstjenester, bør det vurderes tiltak som reduserer risikoen for misbruk i nære relasjoner. Dette kan omfatte løsninger som gjør det mulig å gi andre begrenset tilgang basert på egen eID, fremfor å benytte andres identitet. Slike løsninger kan bidra til å styrke både sikkerhet og sporbarhet ved bruk av eID-tjenester.

Følgende risikoreduserende tiltak retter seg primært mot relevante myndigheter, virksomheter med samfunnssikkerhetsansvar, samt tilbydere av ekomnett- og tjenester:



[36] https://www.finanstilsynet.no/publikasjoner-og-analyser/svindel-og-svindelstatistikk/2025/h1/svindelstatistikk-forste-halvar-2025/

[37] Nedgang i tradisjonell telefonsvindel - Nkom

[38] (EU) nr. 910/2014

[39] ekomforskriften § 9-5

[40] ekomforskriften §§ 1-8 og 1-9 40

[41] https://www.unodc.org/unodc/en/organized-crime/global-fraud-summit/

DIGITAL SVINDEL

Risikoreduserende
TILTAK

- Innhente informasjon om situasjonsbildet for digital svindel.
- Øke bevisstheten i befolkningen om svindelformer og de økonomiske, psykologiske og samfunnsmessige konsekvensene av svindel.
- Øke bevisstheten om risikoen for redusert tillit til ekomtjenester, som kan føre til mer tidkrevende alternativer og digital ekskludering.
- Legge til rette for kombinert blokkering av mobil- og fastnettnumre for å redusere misbruk.
- Styrke beskyttelsen av SMS-avsendernavn.
- Følge opp krav til entydig identifisering av sluttbrukere.
- Kartlegge rammer for deling av informasjon mellom ekom-sektoren og andre sektorer.
- Videreføre dialog og erfaringsutveksling gjennom Nasjonal ekspertgruppe mot digital svindel og internasjonale fora.
- Etablere ordning for delegert tilgang: Det bør utvikles løsninger som gjør det mulig for personer å få tilgang til tjenester på vegne av andre (for eksempel i hjelpe- eller vergeforhold), men hvor den som utfører handlingen benytter egen eID. Dette vil styrke sporbarhet, redusere risiko for misbruk og bidra til tydelig ansvarsfordeling.

2.5 VERDI- OG LEVERANDØRKJEDER

Verdi- og leverandørkjeder i sektoren kan være komplekse og lite oversiktlige. Manglende kontroll og innsikt gjør dem sårbare for påvirkning fra trusselaktører, som kan utnytte slike svakheter til å tilegne seg informasjon, påvirke drift eller i ytterste konsekvens få kontroll over systemer og infrastruktur.

Sårbarheter i leverandørkjeder løftes frem både i Totalberedskapsmeldingen[42] og i rapporten fra Totalberedskapskommisjonen[43]. Næringslivet har en sentral rolle i totalforsvaret fordi mye av infrastrukturen, varene og tjenestene er privat eid. Dette gjelder også ekomsektoren, datasenternæringen og tillitstjenester knyttet til eID. Dette forsterker behovet for at leverandører ikke bare har kontroll på egne systemer og sikkerhetsprosesser, men også har tilstrekkelig innsikt i og oppfølging av sine underleverandører. Underleverandører kan representere en vesentlig sårbarhet dersom deres sikkerhetsnivå ikke er tilstrekkelig ivaretatt. Manglende oversikt over hele leverandørkjeden kan dermed åpne for at trusselaktører utnytter svakheter hos mindre synlige aktører. Dette kan gi uvedkommende tilgang til kritisk informasjon, eksempelvis informasjon om lokasjoner, infrastruktur eller andre skjermingsverdige forhold. For å redusere denne risikoen er det avgjørende med tydelige sikkerhetskrav, systematisk oppfølging og en helhetlig forståelse for risiko på tvers av hele leverandørkjeden.

Kompleksiteten i verdi- og leverandørkjedene forsterkes ytterligere av sektorens avhengighet av spesialisert personell og kompetanse. Flere analyser peker på et økende kompetansegap innen digitale og teknologiske fagområder i Norge, samtidig som behovet for slik kompetanse øker. Dette kan føre til økt avhengighet av et begrenset antall nøkkelpersoner og av utenlandsk personell hos både leverandører og underleverandører. I flere tilfeller vil personell ha behov for sikkerhetsklarering for å kunne utføre oppgaver knyttet til kritisk infrastruktur og sensitive systemer. Klareringsprosessen kan være tidkrevende og dermed påvirke virksomhetenes evne til å dekke kompetansebehov og opprettholde nødvendig kapasitet.

Sårbarheter i leverandørkjeden

I stedet for å angripe godt sikrede virksomheter direkte, kan trusselaktører rette angrep mot underleverandører lenger ut i verdikjeden. Manglende oversikt over leverandøravhengigheter og sikkerhetsnivå i verdikjeden kan bidra til at sårbarheter ikke identifiseres eller håndteres tilstrekkelig. Dette kan gi uautoriserte aktører tilgang til virksomhetskritiske systemer eller data over tid uten å bli oppdaget. Et eksempel på dette er et datainnbrudd hos underleverandører til en norsk teletilbyder, der angripere fikk tilgang til deler av IT-miljøet og senere lekket kunde- og virksomhetsdata. Selskapet opplyste at innbruddet berørte et miljø som var under migrering til nye løsninger, og at det i en periode var uklart hvor omfattende tilgangen hadde vært. I dette tilfellet var det heldigvis ikke snakk om sensitive kundeopplysninger eller operative data. Hendelsen illustrerer likevel hvordan begrenset oversikt over verdikjeden og utilstrekkelig kontroll med data, avhengigheter og leverandører kan føre til alvorlige sikkerhetsbrudd, datalekkasjer og økt risiko for videre kompromittering av kritiske tjenester.

Disse overordnede sårbarhetene kommer særlig til uttrykk gjennom konsentrasjon av kritiske verdier, avhengighet av spesialisert maskin- og programvare, tilgang på nødvendig kompetanse og den økende betydningen av datasentre som kritisk støtteinfrastruktur. De følgende underkapitlene utdyper disse forholdene og deres betydning for risikobildet i sektoren.

2.5.1 Konsentrasjonsrisiko

Konsentrasjonsrisiko oppstår blant annet når flere tilbydere har kritisk utstyr og verdier samlet innenfor et begrenset geografisk område, eksempelvis i datasentre. Dette kan omfatte infrastruktur for drift og styring av ekomnett, tjenesteproduksjon og trafikkutveksling mellom nett. Risikoen forsterkes ytterligere dersom flere sektorer er avhengige av samme lokasjon, eller dersom systemer med ulik kritikalitet er samlokalisert. Lokasjonens betydning og sårbarhet vil derfor i stor grad være knyttet til hvilke aktører og samfunnsfunksjoner som er avhengige av den.

NSM advarer i Risiko 2026[44] om at konsentrasjonsrisiko også kan oppstå gjennom avhengighet til én leverandør eller leverandører fra samme land, noe som kan utnyttes av trusselaktører. Dette understøttes av utviklingstrekk beskrevet i Fokus 2026[45], hvor økende globale avhengigheter og kontroll over kritisk infrastruktur fremheves som strategiske sårbarheter.

Sårbarheten knyttet til en lokasjon avhenger av hvilke kunder, virksomheter og samfunnsfunksjoner som er avhengige av infrastrukturen der. Høy konsentrasjon av kritiske funksjoner kan medføre et betydelig konsekvenspotensial ved sikkerhetstruende hendelser eller andre typer bortfall.

2.5.2 Avhengighet til spesialisert maskinvare og programvare

Sektoren er avhengig av spesialisert maskinvare og programvare. Reservedeler til eldre systemer kan være vanskelige å skaffe dersom de ikke finnes på lager, og enkelte tilbydere samarbeider derfor om tilgang på utstyr. Eldre («legacy») systemer kan i tillegg ha begrensede oppgraderingsmuligheter og dermed økt sårbarhet.

Produksjon av teknologikomponenter, særlig avansert elektronikk, er ofte konsentrert i få geografiske områder. Geopolitisk uro og konflikter kan derfor påvirke forsyningslinjene og tilgangen til kritiske komponenter. Samtidig utfordres «just-in-time»-leveranser når globale forsyningskjeder forstyrres, noe som kan få konsekvenser for drift og beredskap.

Høy grad av spesialisering og stort kapitalbehov gjør at få leverandører tilbyr kritiske systemer. Feil i programvare kan derfor ramme flere tilbydere samtidig. Økende virtualisering og programvaredefinert styring av ekomnett innebærer også større avhengighet av tredjepartsleverandører av IT-løsninger og kan introdusere nye sårbarheter.

2.5.3 Tilgang på kvalifisert teknisk personell

Tilgang på kvalifisert teknisk personell er avgjørende for drift og tjenesteproduksjon. Samtidig peker analyser på et økende kompetansegap innen digitale og teknologiske fagområder i Norge[46]. I et totalforsvarsperspektiv kan personell i samfunnskritiske funksjoner gis fritak fra oppmøte i Forsvaret ved krig, når krig truer og ved styrkeoppbygging. Dette kan bidra til å sikre nødvendig bemanning for å opprettholde drift av kritisk infrastruktur, herunder datasentre, ekomnett og -tjenester. Samtidig gir bemanningsutfordringer i normal drift ikke grunnlag for slikt fritak. I slike tilfeller må den enkelte selv søke om utsettelse av tjeneste.

Dette understreker behovet for at virksomheter har oversikt over kritisk kompetanse og iverksetter tiltak for å sikre tilstrekkelig bemanning både i normalsituasjoner og ved økt beredskap.


Foto: Gunstein Myhre

> *“*
> ***I krisesituasjoner er særlig prinsippene om tilgjengelighet, integritet og konfidensialitet avgjørende for å opprettholde en robust og pålitelig ekominfrastruktur.***

2.5.4 Datasenter som kritisk støtteinfrastruktur

Datasenternæringen er en kritisk støtteinfrastruktur og ble i 2025 underlagt regulering gjennom den nye ekomloven. Dette tydeliggjør kravene til forsvarlig sikkerhet og etablerer et mer helhetlig tilsyns- og beredskapsregime.

Ved utgangen av august 2026 var det registrert 71 datasenteroperatører med til sammen 112 datasentre i Norge. Tallet omfatter både kommersielle og virksomhetsinterne datasentre. Datasentre er nå også omfattet av tilsvarende varslingsplikt som øvrige aktører i ekomsektoren, noe som styrker myndighetenes situasjonsforståelse og evne til koordinert håndtering av uønskede hendelser.

Datasentre utgjør en sentral del av den digitale infrastrukturen ved å sikre lagring, behandling og tilgjenggjøring av data for både offentlige og private aktører. I krisesituasjoner er særlig prinsippene om tilgjengelighet, integritet og konfidensialitet avgjørende for å opprettholde en robust og pålitelig ekominfrastruktur. Samtidig er datasentre avhengige av både ekom og kraft. Avbrudd i disse tjenestene kan få betydelige konsekvenser for kommunikasjon, handel og samfunnssikkerhet.

2.5.5 Vurderinger og risikoreduserende tiltak

Nkom vurderer at sårbarheter i verdi- og leverandørkjeder i økende grad påvirkes av den geopolitiske utviklingen. Økt rivalisering mellom stater kan medføre redusert tilgang til kritisk utstyr, programvare og kompetanse, noe som kan utfordre drift og beredskap i ekomsektoren og datasenterbransjen. Samtidig gjør komplekse og lite oversiktlige leverandørkjeder det krevende å opprettholde tilstrekkelig kontroll over avhengigheter og risikofaktorer.

Sårbarhetene knyttet til konsentrasjon av kritiske verdier, avhengighet av spesialisert maskin- og programvare, tilgang på kompetanse og datasentrenes rolle som kritisk støtteinfrastruktur forsterker hverandre. Dette øker konsekvenspotensialet ved bortfall av enkeltkomponenter, leveranser eller funksjoner, og understreker behovet for økt bevissthet rundt egne avhengigheter og sårbarheter.

Følgende risikoreduserende tiltak retter seg primært mot relevante myndigheter, virksomheter med samfunnssikkerhetsansvar, samt tilbydere av ekomnett- og tjenester:

---

[42] Totalberedskapsmeldingen: Forberedt på krise og krig - regjeringen.no
[43] NOU 2023: 17
[44] https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2026
[45] https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus2026_innhold
[46] https://www.kompetansebehovsutvalget.no/uploads/ryOX1yAG/Kompetansebehovsutvalget_rapport_digitalversjon.pdf

Risikoreduserende TILTAK

- Etablere og vedlikeholde oversikt over egne verdi- og leverandørkjeder, inkludert nasjonale og internasjonale avhengigheter.
- Tilbydere må ha god oversikt over verdikjeder og leverandørkjeder, samt stille tydelige sikkerhetskrav til underleverandører.
- Utvikle og bruke sikre protokoller.
- Etablere strenge kontroll-mekanismer for tilgang.
- Identifisere kritiske komponenter, systemer og innsatsfaktorer som er nødvendige for drift og tjenesteproduksjon.
- Redusere sårbarhet knyttet til konsentrasjon ved å spre kritiske funksjoner og verdier.
- Vurdere tiltak for å håndtere avhengighet til spesialisert maskin- og programvare, herunder tilgang til reservedeler og håndtering av «legacy»-systemer .
- Sikre tilstrekkelig kompetanse for drift og vedlikehold av kritisk infrastruktur.
- Ivareta helhetlig sikkerhet og beredskap i datasentre, med vekt på tilgjengelighet, integritet, autentisitet og konfidensialitet.
- Datasenteroperatører må oppfylle krav til forsvarlig sikkerhet og beredskap, med fokus på sikring og varsling.
- Raskere behandling av sikkerhets- og tilgangs-klareringer.


Foto: Canva

2.6 PLANLAGT ARBEID

2.6.1 Programvare, maskinvare og støttesystemer

Programvare, maskinvare og støttesystemer krever jevnlig oppgradering og vedlikehold. Ved planlagt arbeid kan det oppstå feil som reduserer tilgjengeligheten til tjenester.

Feil i støttesystemer og maskinvare kan forplante seg til høyere nettverkslag og påvirke logiske funksjoner, og i ytterste konsekvens tilgang til tjenester i mobil- og fastnett. Tilstrekkelig redundans i støttesystemer, maskinvare og nettelementer er derfor avgjørende.

Oppbygningen av både fastnett og mobilnett blir stadig mer kompleks, blant annet fordi tradisjonelle IT-systemer i økende grad benyttes til drift og tjenesteproduksjon. Kjernenett kan bestå av komponenter fra flere leverandører, noe som gjør det mer krevende å ha oversikt over avhengigheter og konsekvenser ved endringer. Tette koblinger mellom systemer og grensesnitt gjør også at feil kan spre seg raskt til større deler av infrastrukturen.

Mobilnett er særlig komplekse og avhengige av konsistens og synkronisering på tvers av nettelementer og instanser, både i kjernenettet, radionettet og i forbindelsene mellom disse. Denne kompleksiteten øker risikoen for konfigurasjonsfeil.

Eksponering av posisjonsdata i mobilnettet

Den 20. mars 2026 oppdaget en ansatt hos sikkerhetsselskapet Mnemonic, i samarbeid med NRK, et sikkerhetshull hos Telia. Telia ble varslet om forholdet 13.april, og sårbarheten ble lukket natt til 14.april.

NRK demonstrerte sikkerhetshullet ved å spore Høyre-politiker Peter Frølichs posisjon. Journalisten kunne blant annet fastslå at Frølich befant seg på Stortinget, samt beskrive reiseruten han hadde benyttet fra hjemmet til Stortinget samme morgen.

Sikkerhetshullet oppstod som følge av en konfigurasjonsfeil i 2023. Fram til feilen ble rettet 14.april 2026, var informasjon om hvilken basestasjon en bruker var tilkoblet tilgjengelig i datastrømmen som ble sendt til mobilhåndsettet.

Feilen var knyttet til hvordan Telias nett håndterte Session Initiation Protocol (SIP), kommunikasjonsprotokollen som brukes av VoLTE – taleanrop over 4G. Utnyttelse av sårbarheten krevde ingen hacking, men kunne gjennomføres ved å lese av informasjon som ble overført ved et ordinært taleanrop. Sårbarheten berørte håndsett tilknyttet bedriftsplattformtjenestene SmartConnect og Bedriftsnett. Konfigurasjonsfeilen medførte at Cell-ID ikke ble fjernet fra SIP-pakken før den ble sendt til håndsettene. Ved hjelp av offentlig tilgjengelige databaser og oppslagstjenester kunne Cell-ID benyttes til å identifisere hvilken basestasjon brukeren var tilkoblet, og dermed gi informasjon om vedkommende geografiske lokasjon.

2.6.2 Planlagt utfasing av 2G

Slukkingen av 2G-nettene er en naturlig del av den teknologiske utviklingen i ekomnettene. Overgangen fra 2G til 4G- og 5G-teknologi vil gi bedre og sikrere tjenester. I tillegg gir 4G- og 5G-teknologi en mer effektiv og bærekraftig utnyttelse av ressurser. Samtidig kan utfasing av eldre teknologi og overgang til nye løsninger medføre sårbarheter dersom funksjonalitet og avhengigheter ikke ivaretas er tilstrekkelig. Et teknologiskifte som slukking av 2G-nettene vil føre med seg utfordringer for brukere som er avhengige av utstyr basert på 2G-teknologi. Dette gjelder spesielt for signaloverføring for maskin-til-maskin kommunikasjon, og kan berøre alt fra heisalarmer og eCall til overvåking av ustabile fjellområder. Dersom utstyr som er avhengig av 2G-teknologi ikke skiftes ut før 2G-nettene slukkes, vil både utstyret og de tilhørende tjenestene slutte å fungere.

2.6.3 eID og tillitstjenester

For eID og tillitstjenester medfører eIDAS 2.0 økt teknologisk kompleksitet, særlig som følge av innføringen av EUDI Wallet og nye tilhørende tjenester. Erfaringer fra ENISAs årsrapporter de siste to årene viser at systemfeil, herunder programvare- og maskinvarefeil, utgjør hovedandelen av de rapporterte hendelsene. Økt kompleksitet øker sannsynligheten for slike feil, og konsekvensene kan være tjenesteavbrudd, redusert tilgjengelighet og svekket tillit til tjenestene[47].

Varslede hendelser til Nkom viser tilsvarende utvikling, der hovedandelen av uønskede hendelser skyldes systemfeil der de fleste av disse oppstår i forbindelse med planlagt arbeid. 83 prosent av hendelsene er klassifisert som «betydelig», mens de resterende 17 prosentene er kategorisert som «stor påvirkning». Hendelsene i sistnevnte kategori skyldtes globale problemer i Microsofts Azure-tjeneste 29. oktober 2025. Når store, globale tjenester opplever uventet nedetid over flere timer, kan dette få omfattende konsekvenser for underliggende systemer.

EUDI Wallet-løsninger er fortsatt under utvikling[48], og innføringen av nye teknologier bidrar til å øke systemenes angrepsflate. Sårbarheter kan oppstå i overgangsperioder der løsninger er under utvikling eller kun delvis implementert, samtidig som både systemeiere og brukere har begrenset erfaring med de nye løsningene. En økt angrepsflate gir flere potensielle inngangspunkter for angripere, og den økte kompleksiteten kan gjøre det mer krevende å avdekke og håndtere sikkerhetshull på tvers av komponenter og integrasjoner.

2.6.4 Vurderinger og risikoreduserende tiltak

Nkom vurderer at det er utfordrende å ha full oversikt over risikoen knyttet til komplekst planlagt arbeid. Konfigurasjonsendringer kan få uventede ringvirkninger som først blir synlige etter at endringene er gjennomført. I slike tilfeller kan det være nødvendig å rulle tilbake endringene. Det er derfor viktig å ha gode rutiner for risikovurdering av planlagt arbeid, samt å ha tilstrekkelige rutiner for testing og tilbakeføring av endringer ved behov for å gjenopprette den opprinnelige konfigurasjonen.

> *“*
> ***Når store, globale tjenester opplever uventet nedetid over flere timer, kan dette få omfattende konsekvenser for underliggende systemer.***

Nkom gjennomfører jevnlig tilsyn med tilbydere etter hendelser knyttet til planlagt arbeid. Resultatene fra tilsynene viser at mangelfulle eller feilslåtte risikovurderinger ofte går igjen. De fleste hendelsene har sin bakgrunn i organisatorisk eller menneskelige feil, snarere enn teknisk svikt. Andre årsaker omfatter komplekse leverandørkjeder med fragmentert ansvar og manglende helhetlige risikovurderinger.

Ved utsetting av IT-systemer og bruk av tredjeparter til levering av nettverksfunksjoner er det viktig å gjennomføre risikovurderinger for å vurdere konsekvenser for driftsstabilitet, kontroll og sikkerhet. Det bør også gjennomføres tilstrekkelig testing og verifikasjon i isolerte miljøer før endringer settes i produksjon. Det er videre viktig å prioritere analyse og oppfølging av varsler fra kontrollsystemer. Flere større sikkerhetshendelser har i ettertid vist at kontrollsystemer varslet om avvik på et tidlig tidspunkt, uten at dette ble fanget opp. Tidlig identifisering og håndtering av slike varsler kan bidra til å begrense skadeomfanget og i enkelte tilfeller forhindre sikkerhetshendelser.

Når det gjelder den planlagte utfasingen av 2G-nettene innen utgangen av 2027, vurderer Nkom at det er nødvendig å legge til rette for en smidig og kontrollert overgang til nyere teknologi. Dette forutsetter tett oppfølging og kontinuerlig dialog med de aktuelle mobiloperatørene.

Arbeidet med å erstatte 2G-avhengig utstyr med løsninger som støtter 4G og 5G må intensiveres i tiden frem mot utfasingstidspunktet. Nkom vurderer det som særlig viktig at myndighetene, i samarbeid med tilbydere og

PLANLAGT ARBEID

> *“*
> ***De fleste hendelsene har sin bakgrunn i organisatorisk eller menneskelige feil, snarere enn teknisk svikt.***



Foto: Getty

øvrige berørte aktører, samordner og forsterker informasjonsarbeidet.

Revisjonen av eIDAS må ses i sammenheng med økt avhengighet av felles europeisk digital infrastruktur. Kritiske funksjoner i felleskomponenter, som EUDI Wallet, som skal benyttes på tvers av landegrenser, medfører en avhengighet av en robust og pålitelig digital infrastruktur. Overgangen til det reviderte regelverket er sammensatt og preget av uavklarte krav og økt teknisk kompleksitet. Helhetlig risikohåndtering er derfor viktig i overgangsfasen, frem til rettsakter, implementeringsstandarder og operasjonell erfaring er fullt etablert. Virksomhetene må arbeide strukturert og proaktivt for å redusere sårbarheter og sikre etterlevelse.

Følgende risikoreduserende tiltak retter seg primært mot relevante myndigheter, virksomheter med samfunnssikkerhetsansvar, samt tilbydere av ekomnett- og ekomtjenester:


Foto: Gunstein Myhre

[47] https://www.enisa.europa.eu/sites/default/files/2024-12/2023_Trust_Services_Incident_Reporting_week50-2024_en_10.12.2024.pdf

[48] https://www.eudi-wallet.eu/

PLANLAGT ARBEID

Risikoreduserende TILTAK

- Sikre at alt planlagt arbeid må følge etablerte prosedyrer og sikkerhetskrav for å unngå utilsiktede driftsforstyrrelser.
- Gjennomføre grundige risikovurderinger før planlagt arbeid for å identifisere mulige konsekvenser og nødvendige risikoreduserende tiltak.
- Teste endringer grundig før implementering og gjennomføre evalueringer og revisjoner for å lære av feil og forbedre prosesser.
- Sørge for at risiko- og sårbar-hetsvurderinger er oppdaterte og dekker alle relevante aspekter ved arbeidet.
- Etablere og vedlikeholde fungerende reserveløsninger for kritiske tjenester, slik at feil ikke fører til omfattende tjenesteutfall.
- Gjennomføre jevnlige revisjoner av underleverandører for å sikre at de oppfyller krav til sikkerhet, beredskap og kvalitet.
- Etablere tydelige rutiner for rask og presis varsling til relevante myndigheter og interessenter ved avvik under planlagt arbeid.
- Benytte styringssystemer og systemer for kvalitetssikring i forbindelse med planlagt arbeid.
- Gjennomføre sidemannskontroll ved endringer med stort konsekvenspotensial.
- Etablere og vedlikeholde rutiner for tilbakerulling av endringer.
- Teste tilbakerulling av endringer og gjennomføre tilstrekkelig testing før produksjonssetting i nettet.
- Benytte infrastruktur som kildekode (Infrastructure as Code).
- Gjennomføre planlagt arbeid på tidspunkter der konsekvensene av eventuelle feil forventes å være minst mulig.
- Arbeide systematisk med å opprettholde og videreutvikle systemkunnskap for å forstå hvordan konfigurasjonsendringer påvirker systemer og hvordan feiltilstander kan oppstå.
- Etablere og gjennomføre målrettet informasjonsarbeid om utfasing av 2G-nettene innen 2027, med tydelig budskap om at alt 2G-avhengig utstyr må identifiseres og erstattes i god tid før slukking.
- Etablere overvåking, avviks-håndtering og hendelsesrespons for eID-løsninger og tillits-tjenester som dekker både nye og eksisterende komponenter.
- Innføre trinnvis og kontrollert implementering av eID-løsninger og tillitstjenester, med særlig vekt på testing, verifikasjon og pilotering.
- Gjennomføre systematiske trussel- og sårbarhetsanalyser for eID-løsninger og tillitstjenester, med særskilt fokus på overgangsperioder.



2.7 NATURHENDELSER

Ifølge Meteorologisk institutt kan Norge i årene fremover forvente økende temperaturer og mer nedbør over hele landet. Dette innebærer økt sannsynlighet for episoder med kraftig styrtregn, flom, skred og sterk vind. Ekstremvær vil også i større grad kunne ramme områder som historisk sett har vært mindre utsatt for slike hendelser.

Utviklingen de siste årene viser allerede en tydelig tendens. Siden 2023 har det hvert år forekommet minst to ekstremværhendelser som i større eller mindre grad har slått ut elektronisk kommunikasjon med varierende konsekvenser og varighet (Se figur 5).

2.7.1 Ekstremvær

Et eksempel på ekstremvær med store konsekvenser er ekstremværet Amy i oktober 2025. Hovedårsaken til ekomutfallene var brudd i strømforsyningen som følge av lokale kraftutfall. På det meste var om lag 155 000 husstander uten strøm. Dette førte til bortfall av nær 1 600 ordinære basestasjoner hos ulike tilbydere, samt 133 basestasjoner i Nødnett. Enkelte områder sto helt uten kommunikasjonsmuligheter over lengre perioder. Tilsvarende utfordringer oppstod også i romjulen 2025.

Økende temperaturer gir hyppigere perioder med kraftig nedbør, der særlig korttidsnedbøren forventes å øke. Intense nedbørsmengder, tung snø og rask snøsmelting kan føre til flom, overvann og oversvømmelser i byer og tettsteder. Dette vil kunne føre til skader på ekominfrastruktur og økt risiko for tjenesteutfall. Ekominfrastruktur er også sårbar for skred.



Figur 5 Ekstremvær og store ekomutfall i Norge, 2023 - 2025


Foto: Nkom

Infrastruktur går ofte gjennom skredutsatte områder, og skred kan skade både nedgravde fiberkabler, fiber i luftspenn, basestasjoner og nodehytter. I tillegg kan skred utgjøre en fare for entreprenører som skal rette feil i området, noe som kan forsinke gjenoppretting av tjenester.

2.7.2 Brann

Skogbranner og større branner i Norge har historisk sett vært av begrenset omfang, men risikoen øker i perioder med høy temperatur og tørke. Særlig sørlige og sørøstlige delene av landet er utsatt. Brann i sentraler og anlegg som inngår i ekominfrastrukturen kan få alvorlige konsekvenser dersom hendelsen ikke oppdages og håndteres raskt. Erfaringene fra blant annet brannen i Lærdal i 2014 viste hvordan omfattende brannhendelser kan påvirke ekomtjenester og utfordre samfunnets kommunikasjonsevne. Selv om tilbydere har krav til brannsikring, kan brann som følge av både tekniske feil, menneskelige handlinger og ytre påvirkninger få alvorlige konsekvenser for ekominfrastrukturen. Ekstreme værforhold, som langvarig varme og tørke, kan i tillegg øke sannsynligheten for slike hendelser.

2.7.3 Romvær

Romvær refererer til aktivitet i solens atmosfære, som solstormer og koronamasseutbrudd. Slike hendelser kan påvirke satellittsystemer, kraftnett og kommunikasjonssystemer. Solstormaktiviteten følger statistisk en syklus på omtrent elleve år, men store enkelthendelser kan også inntreffe utenom periodene med høyest aktivitet. Et eksempel er solstormen i 1989 som blant annet lammet kraftforsyningen i Quebec i Canada.

Samlet sett viser utviklingen at ekstremvær i økende grad påvirker ekom. Hyppigere og mer intense hendelser gir både flere utfall og lengre gjenopprettingstid, særlig når feil skyldes bortfall av strøm, skred eller skader på kritisk infrastruktur.

2.7.4 Vurderinger og risikoreduserende tiltak

En grunnleggende utfordring er at ekom–infrastruktur ofte er etablert i områder utsatt for flom og skred. I mange tilfeller følger infrastrukturen traseer langs annen kritisk infrastruktur, som vei og kraft. Dette gjør omlegging krevende og kostbart. Likevel vurderer Nkom at tilbydere i flere tilfeller kan gjennomføre risikoreduserende tiltak knyttet til naturhendelser.

Ekomsektoren har betydelige avhengigheter til kraftforsyning, og bortfall av kraft kan få konsekvenser for ekominfrastruktur over store geografiske områder. Ved langvarige strømbrudd vil mobilnettene normalt falle ut etter 2–4 timer når reservestrømmen ved basestasjonene er oppbrukt. Bredbåndsnett og trådløse nettverk vil som regel bli utilgjengelige umiddelbart dersom sluttbrukeren ikke har reservestrøm til modem, ruter og annet nettverksutstyr. I tillegg kan enkeltbrudd på fiberkabler føre til umiddelbart bortfall av mobil- og bredbåndstjenester i avgrensede områder. Erfaringer fra håndtering av ekstremværshendelser har vist forbedret samarbeid og koordinering mellom kraft- og ekomsektoren. Slike erfaringer vurderes også som relevante for å styrke håndteringsevnen ved tilsiktede hendelser, herunder sabotasje.

Tiltak som sikrer tilstrekkelig reservestrøm, vil kunne redusere risikoen for omfattende regionale utfall og bør derfor prioriteres høyt.

Virksomheter og offentlige etater kan også iverksette tiltak for å gjøre tjenestene mer robuste ved bortfall av ekom. Det kan blant annet være hensiktsmessig å etablere oppmøtesteder i kommunen der innbyggere kan motta viktig informasjon og eventuelt få tilgang til nødkommunikasjon. Prioritetsabonnement kan bidra til å opprettholde kritiske kommunikasjons–linjer ved høy belastning, eller så lenge ett av mobilnettene er tilgjengelig. Dual-SIM-løsninger kan gi bedre dekning og alternative forbindelser ved nettutfall.

Når det gjelder romvær, bør systemer for overvåking og varsling være tilgjengelige og brukervennlige for relevante aktører. Selv om Nkom ikke har direkte ansvar for slike systemer, er tett dialog med institusjonene som overvåker romvær viktig. Dette gjelder særlig Meteorologisk institutt, Norsk Romsenter og Universitetet i Tromsø.

For offentlige etater, statsforvaltere og kommuner har satellittelefoner lenge vært et sentralt beredskapsverktøy for nødkommunikasjon. Det satses nå bredt på bruk av både geostasjonære satellitter og lavbanesatellitter som transmisjonsbærere. Offentlige aktører og nødetater vil derfor i økende grad bli avhengige av satellitt som reservekommunikasjon, noe som også må ses i sammenheng med systemer for overvåking og varsling.

Følgende risikoreduserende tiltak retter seg primært mot relevante myndigheter, virksomheter med samfunnssikkerhetsansvar, samt tilbydere av ekomnett- og tjenester:

Risikoreduserende
TILTAK

- Gjennomføre fysisk sikring av kritisk infrastruktur, inkludert flom- og brannsikring.
- Etablere og dimensjonere tilstrekkelig reservestrøm for kritiske komponenter.
- Etablere tiltak for å opprettholde kommunikasjon ved bortfall av ekom, herunder oppmøtesteder og nødkommunikasjonsløsninger.
- Benytte prioritetsabonnement og dual-SIM-løsninger for økt robusthet i mobilkommunikasjon.
- Sikre tilgang til og aktiv bruk av systemer for overvåking og varsling av romvær.
- Etablere tett samarbeid med relevante fagmiljøer innen vær- og romværsovervåking.
- Vurdere og ta i bruk satellittbasert reservekommunikasjon i offentlig sektor og hos nødetater.

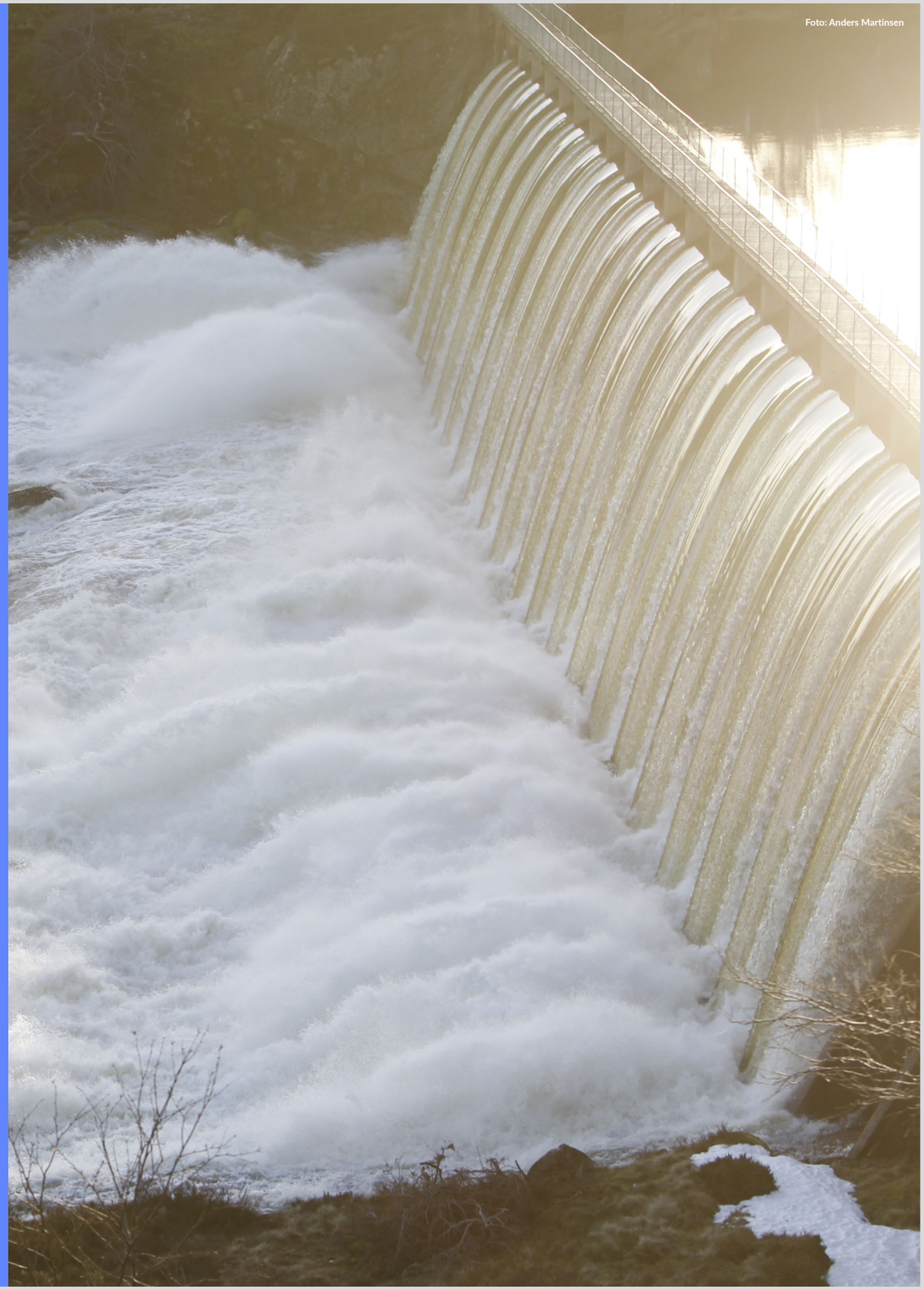
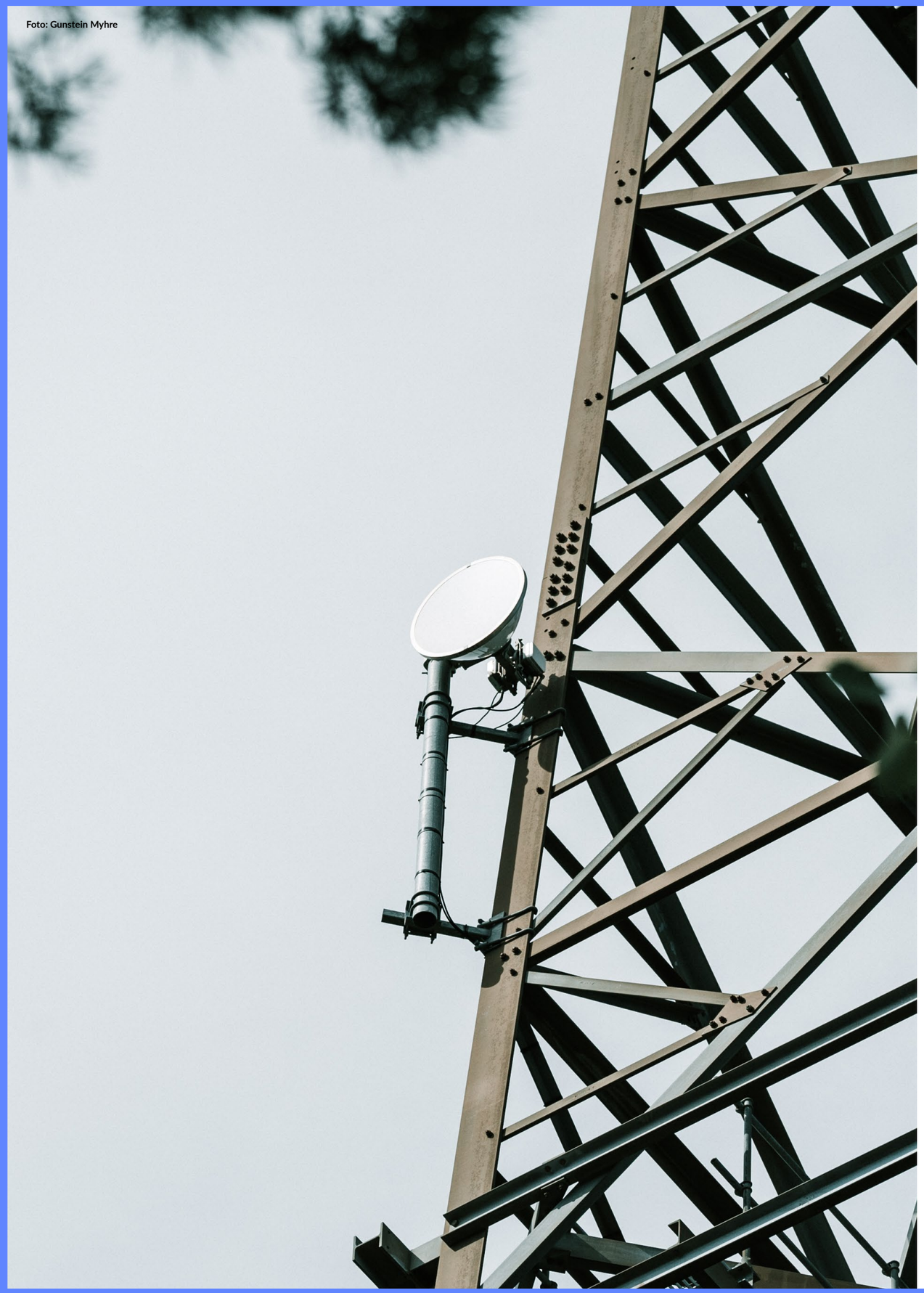


Foto: Anders Martinsen

Foto: Gunstein Myhre



3 NKOMS EGENBEREDSKAPSRÅD OG OPPSUMMERING

For å styrke samfunnets motstandskraft ved bortfall eller svikt i elektroniske kommunikasjonstjenester har Nkom utarbeidet egne råd om egenberedskap knyttet til ekom. Disse rådene presenteres først i dette kapittelet.

Deretter gis en oppsummering av sentrale tiltak fra kapittel 3 (farer, trusler og sårbarheter i sektoren) som bidrar til å styrke robustheten og beredskapen i ekomsektoren.

Myndighetenes egenberedskapsråd for ekom

Finn ut hvordan kommunen informerer
Sjekk om kommunen vil etablere informasjonspunkter, eller har andre planer for å dele viktig informasjon ved større problemer med mobilnett eller internett.

Vær en beredskapsvenn
Digitale tjenester gjør oss mer sårbare – samarbeid gjør oss sterkere. Finn ut hvem du kan hjelpe, hvem du kan få hjelp av, og hvilket utstyr dere kan dele. Bli enige om hvor dere skal møtes dersom dere ikke får kontakt med hverandre.

Skaff en DAB-radio
DAB-radio bruker et eget kringkastingsnett. Med en DAB-radio som går på batterier, solceller eller sveiv kan du få viktig informasjon fra myndighetene selv om internett er nede. De fleste biler har også DAB-radio.

Lad opp batteribank og utstyr
Ha en oppladet batteribank tilgjengelig, og ekstra batterier til radioen. Ved fare for problemer med mobilnett, internett eller strøm; lad mobil, datamaskin og annet utstyr. Mobilen kan fortsatt være nyttig, for eksempel som lommelykt, eller når dekningen kommer og går.

Vurder abonnement med ulike mobilnett
Ha en beredskapsvenn, eller noen i din omgangskrets, med abonnement som bruker et annet mobilnett enn det du har. Da mister ikke alle dekningen samtidig dersom det oppstår feil i ett av mobilnettene. Mange mobiltelefoner har også mulighet for å ha to eller flere SIM-kort/eSIM.

Finn ut hvordan du kan kommunisere over wifi
Hvis mobilnettet er nede, kan du fortsatt ringe eller kommunisere på andre måter over internett. Sjekk om telefonen din støtter wifi-anrop, og hvordan du slår på denne funksjonen. Avtal med andre du kjenner hvilke apper dere også kan bruke til samtaler og meldinger, og sjekk at de fungerer.

Sjekk om kommunen har forsterket mobilnett
Mange kommuner har basestasjoner med reservestrøm i opptil tre døgn, ofte i nærheten av kommunehus eller rådhus. Hvis du mister mobildekningen hjemme, kan du dra dit (hvis det er trygt) for å få kontakt med folk.

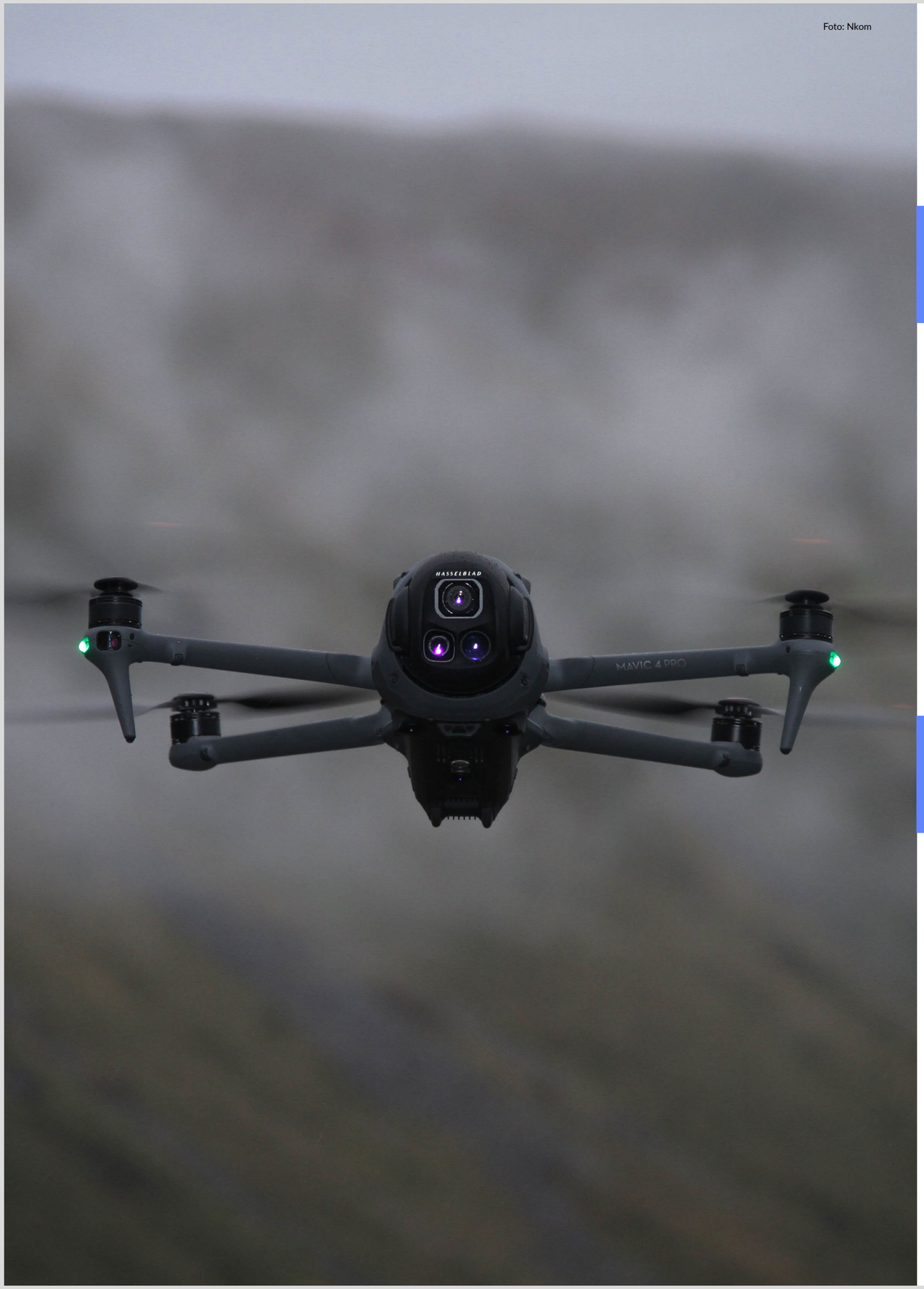


Foto: Nkom

OPPSUMMERING AV ANBEFALTE TILTAK

STATLIGE TRUSLER

Gjennomgå og eventuelt oppdatere planer for beskyttelse av egen infrastruktur.

Kontrollere og kvalitetssikre planer for risikoreduserende tiltak.

Sikre at alle ansatte har tilstrekkelig risiko- og sikkerhetsforståelse i lys av dagens sikkerhetspolitiske situasjon.

Benytte NSMs cybersjekk.no for å kartlegge egen cybersikkerhet.

HA FOKUS PÅ SIKKERHETSSTYRING I ALLE LEDD, HERUNDER:

- Oversikt over verdier og avhengigheter
- Rutiner for oppdatering av programvare
- Begrensning av tilgang og aksess
- Utøve god sikkerhetsledelse, inkludert kjennskap til egne ansatte
- Vurdere bruk av sikkerhetstesting, eksempelvis penetrasjonstesting
- Etablere og vedlikeholde beredskapsplaner for redundans, reserveløsninger og reparasjon etter hendelser

POSISJON, NAVIGASJON OG TID (PNT)

Delta i øvelser som Jammertest for å teste og avdekke sårbarheter i systemer som benytter GNSS og PNT.

Sikre tilstrekkelig redundans i kilder til PNT-informasjon, slik at bortfall i ett system ikke medfører omfattende utfall eller forstyrrelser.

Isolere PNT-kilder fra hverandre, både fysisk og implementeringsmessig, for å hindre at feil i én kilde påvirker andre.

Følge utviklingen innen multi-PNT og alternative PNT-løsninger (APNT), og vurdere implementering der det er hensiktsmessig.

Benytte flere uavhengige GNSS-systemer, herunder europeiske løsninger som Galileo, for å oppnå økt robusthet.

CYBERDOMENET

Følge utviklingen og implementere tilstrekkelige løsninger for håndtering av tjenestenektangrep.

Sikre at transittavtaler og samtrafikkpunkt BGP-avtaler inkluderer mekanismer for håndtering av distribuerte tjenestenektangrep.

Etablere og vedlikeholde mekanismer for sikker ruting.

Innføre overvåking av egne ruteannonseringer for å avdekke avvik eller uautoriserte annonseringer.

Stille tydelige sikkerhetskrav til leverandører og begrense deres tilgang til utviklings- og produksjonsmiljøer.

Etablere rutiner for identifisering og håndtering av sårbarheter, inkludert systematisk oppdatering og overvåking.

Benytte tilgangsstyring, segmentering av nettverk og flerfaktorautentisering for å redusere risiko for uautorisert tilgang.

Etablere sikre reserveløsninger og teste gjenoppretting jevnlig.

Sørge for rask identifikasjon, overvåking og isolering av kompromitterte komponenter og miljøer.

Forankre ansvar for leverandør- og verdikjederisiko i ledelsen og gjennomføre jevnlige risikovurderinger.

Benytte avviks- og atferdsbasert deteksjon, samt prinsippet om minste privilegium og overvåking av kritiske systemer.

Sikre kontrollert og trinnvis innføring av KI-systemer, herunder bruk av pilotering før bred implementering.

Stille krav til dokumentasjon, logging, forklarbarhet og etterprøvbarhet av KI-systemer og beslutninger.

Vurdere regulatorisk etterlevelse og behov for alternative løsninger eller utfasing dersom KI-funksjonalitet ikke kan tilfredsstille gjeldende eller kommende krav.

Utvikle kompetanse om KI i sektoren, med særlig vekt på sikkerhet og risikoforståelse.

DIGITAL SVINDEL

Innhente informasjon om situasjonsbildet for digital svindel.

Øke bevisstheten i befolkningen om svindelformer og de økonomiske, psykologiske og samfunnsmessige konsekvensene av svindel.

Øke bevisstheten om risikoen for redusert tillit til ekomtjenester, som kan føre til mer tidkrevende alternativer og digital ekskludering.

Legge til rette for kombinert blokkering av mobil- og fastnettnumre for å redusere misbruk.

Styrke beskyttelsen av SMS-avsendernavn.

Følge opp krav til entydig identifisering av sluttbrukere.

Kartlegge rammer for deling av informasjon mellom ekomsektoren og andre sektorer.

Videreføre dialog og erfaringsutveksling gjennom Nasjonal ekspertgruppe mot digital svindel og relevante internasjonale fora.

Etablere ordning for delegert tilgang: Det bør utvikles løsninger som gjør det mulig for personer å få tilgang til tjenester på vegne av andre (for eksempel i hjelpe- eller vergeforhold), men hvor den som utfører handlingen benytter egen eID. Dette vil styrke sporbarhet, redusere risiko for misbruk og bidra til tydelig ansvarsfordeling.

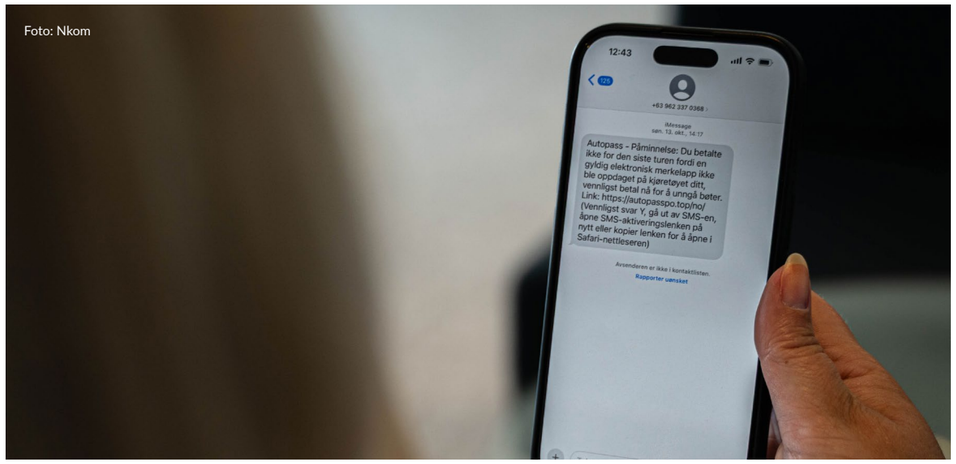


Foto: Nkom

PLANLAGT ARBEID

Alt planlagt arbeid må følge etablerte prosedyrer og sikkerhetskrav for å unngå utilsiktede driftsforstyrrelser.

Før man setter i gang arbeid, skal det gjennomføres en grundig risikovurdering for å identifisere mulige konsekvenser og nødvendige risikoreduserende tiltak.

Endringer må testes grundig før implementering, og det bør gjennomføres evalueringer og revisjoner av arbeidet for å lære av eventuelle feil.

Risiko- og sårbarhetsvurderinger må være oppdaterte og dekke alle relevante aspekter av arbeidet.

Det må være fungerende reserveløsninger for kritiske tjenester, slik at en feil ikke fører til omfattende tjenesteutfall.

Underleverandører må jevnlig revideres for å sikre at de oppfyller kravene til sikkerhet, beredskap og kvalitet.

Det må være tydelige rutiner for rask og presis varsling til relevante myndigheter og interessenter dersom det oppstår avvik under planlagt arbeid.

Benytte styringssystemer og system for kvalitetssikring i forbindelse med planlagt arbeid.

Gjennomføre sidemannskontroll ved endringer som har et stort konsekvenspotensial.

Etablere og vedlikeholde rutiner for tilbakerulling av endringer.

Teste tilbakerulling av endringer og gjennomføre tilstrekkelig testing før produksjonssetting i nettet.

Benytte infrastruktur som kildekode (Infrastructure as Code).

Gjennomføre planlagt arbeid på tidspunkter der konsekvensene ved feil forventes å være minst mulig.

Opprettholde og videreutvikle systemkunnskap for å forstå hvordan konfigurasjons-endringer kan påvirke systemet og hvordan feiltilstander kan oppstå ved konfigurasjon.

Etablere og gjennomføre målrettet informasjonsarbeid om utfasing av 2G-nettet innen 2027, med tydelig budskap om at alt 2G-avhengig utstyr må identifiseres og erstattes i god tid før slukking.

Etablere overvåking, avvikshåndtering og hendelsesrespons for eID-løsninger og tillitstjenester som dekker både nye og eksisterende komponenter.

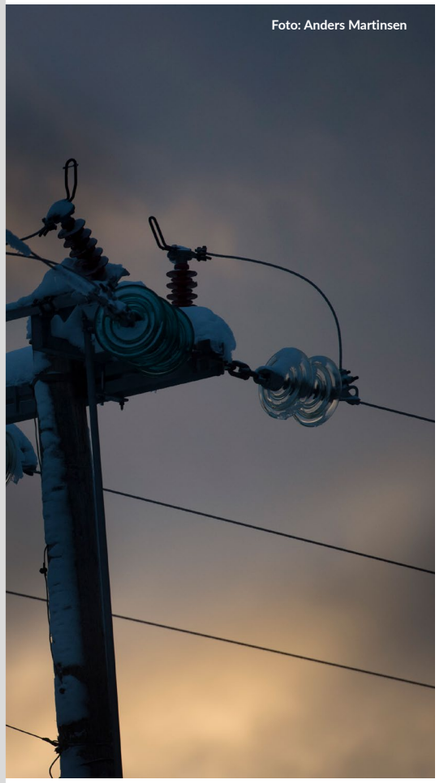
Innføre trinnvis og kontrollert implementering av eID-løsninger og tillitstjenester, med særlig vekt på testing, verifikasjon og pilotering.

Gjennomføre systematiske trussel- og sårbarhetsanalyser for eID-løsninger og tillits-tjenester, med særskilt fokus på overgangsperioder.



Foto: Gunstein Myhre

VERDI- OG LEVERANDØRKJEDER


Foto: Anders Martinsen

Etablere og vedlikeholde oversikt over egne verdi- og leverandørkjeder, inkludert nasjonale og internasjonale avhengigheter.

Tilbydere må ha god oversikt over verdikjeder og leverandørkjeder, samt stille sikkerhetskrav til underleverandører.

Utvikle og benytte sikre protokoller.

Etablere strenge kontroll-mekanismer for tilgang.

Identifisere kritiske komponenter, systemer og innsatsfaktorer som er nødvendige for drift og tjenesteproduksjon.

Redusere sårbarhet knyttet til konsentrasjon ved å spre kritiske funksjoner og verdier.

Vurdere tiltak for å håndtere avhengighet til spesialisert maskin- og programvare, herunder tilgang til reservedeler og håndtering av «legacy»-systemer.

Sikre tilstrekkelig kompetanse for drift og vedlikehold av kritisk infrastruktur.

Ivareta helhetlig sikkerhet og beredskap i datasentre, med fokus på tilgjengelighet, integritet, autentisitet og konfidensialitet.

Oppfylle krav til forsvarlig sikkerhet og beredskap i datasentre, med fokus på sikring og varsling.

Legge til rette for raskere behandling av sikkerhets- og tilgangsklareringer.

NATURHENDELSER

Fysisk sikring av kritisk infra-struktur, inkludert flom- og brannsikring.

Etablere og dimensjonere tilstrekkelig reservestrøm for kritiske komponenter.

Tiltak for å opprettholde kommunikasjon ved bortfall av ekom, herunder oppmøtesteder og nødkommunikasjon.

Benytte prioritetsabonnement og dual-SIM-løsninger for økt robusthet i mobil-kommunikasjon.

Sikre tilgang til og aktiv bruk av systemer for overvåking og varsling av romvær.

Tett samarbeid med relevante fagmiljøer innen vær- og romværsovervåking.

Vurdere og ta i bruk satellittbasert reservekommunikasjon i offentlig sektor og hos nødetater.


Foto: Gunstein Myhre



Foto: Gunstein Myhre

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