Nasjonal kommunikasjons-myndighet

EkomROS 2019:

Den digitale grunnmuren

Risikovurdering av ekomsektoren - Juni 2019

SAMMENDRAG - EkomROS 2019

Nasjonal kommunikasjonsmyndighet (Nkom) har siden 2016 publisert en årlig risikovurdering av den sektoren som tilbyr elektroniske kommunikasjonstjenester og nett i Norge; mobiltelefoni, bredbånd, kringkasting osv. (ekomsektoren). Vurderingen bygger på erfaringer fra faktiske hendelser de siste årene og utviklingstrekk av betydning for sektoren og samfunnet.

I 2018 registerte Nkom 61 hendelser av en viss alvorlighetsgrad. Fiberbrudd er den vanligste årsaken til feil i ekomnett og -tjenester, etterfulgt av programvarefeil, strømutfall og ekstremvær.

I årets EkomROS omtaler vi begrepet «Den digitale grunnmuren». Med dette mener vi nett og tjenester som er avgjørende for at Norge skal være et moderne, trygt og solid samfunn. Grunnmuren må tåle betydelig belastning fordi den bærer en rekke tjenester både for innbyggerne i Norge, næringslivet, samfunnet og brukere som trenger spesielt gode og sikre tjenester. Å sikre denne grunnmuren, må derfor være førende for både myndigheter og næringen som tilbyr tjenester og nett.

I tillegg til erfaringer fra hendelser og kunnskap om avdekte sårbarheter, vurderer Nkom endringene i risikobildet som følge av samfunnsmessige, organisatoriske og teknologiske utviklingstrekk. Nkom samarbeider også tett med Politiets sikkerhetstjeneste, E-tjenesten, Nasjonal sikkerhetsmyndighet (NSM) og med bransjen selv, for slik å dele overordnede situasjonsbilder av styrker og svakheter i beredskapen.

Årets EkomROS peker på følgende tre ***utviklingstrekk*** av betydning de kommende årene:

- *Samfunnsmessig – økt digitalisering. Digitaliseringen skjer i høyt tempo og Norge er allerede et av verdens mest digitaliserte land. Utbredelsen av 5G og IoT står sentralt i den videre digitaliseringen og samfunnsutviklingen. For å sikre fremgang i bruk av digitale tjenester, må brukerne ha tillit til at tjenestene er sikre og alltid tilgjengelige. Dette stiller svært store krav til de ekomnett og -tjenester som skal bære de digitale verdiene;* ***den digitale grunnmuren.***

- *Organisatorisk - nye rammebetingelser. Nytt regelverk for å ivareta samfunnsikkerhet, herunder også sikkerhet i elektronisk kommunikasjon, blir utviklet fortløpende. Ny sikkerhetslov medfører blant annet at virksomheter innen elektronisk kommunikasjon må ta større ansvar for å sikre seg mot angrep som kan skade nasjonale sikkerhetsinteresser. I tillegg vil nytt europeisk regelverk legge føringer for både teknologiutvikling og håndtering av data innen tradisjonelle og nye ekomtjenester.*

- *Teknologisk - forskyvning av kompleksitet. Teknologiutviklingen innenfor ekom går i retning av virtualisering av infrastruktur, flytting av tjenesteproduksjon, lagring i skyen og automatisering ved at kunstig intelligens tar stadig flere beslutninger. Fra virksomhetenes side vil dette kunne bidra til rasjonalisering og forbedring av tjenester til kundene. Samtidig medfører utviklingen lange verdikjeder med stadig flere involverte aktører, og med forskyvning av kompleksitet utover i verdikjeden. Dette utfordrer aktørene når de skal vurdere den samlede sårbarheten og risikoen for produkter og tjenester de tilbyr i markedet.*

Nkom har vurdert risikoer ut fra tre faktorer: verdiene som den digitale grunnmuren skal bære, truslene den digitale grunnmuren utsettes for, og sårbarhetene i sektoren.

- *Verdier - den digitale grunnmuren muliggjør digitalisering i de ulike sektorene. Den digitale grunnmuren er i stadig økende grad bærer av grunnleggende samfunnsverdier som liv og helse, økonomi, samfunnsstabilitet og demokratiske verdier og styringsevne.*

- *Trusler - utilsiktede hendelser som følge av for eksempel ekstremvær og menneskelig feil, vil fortsatt stå for flesteparten av sikkerhetshendelsene i ekomsektoren. Nkom anser imidlertid at trusselaktørenes vilje til å rette oppmerksomhet mot den digitale grunnmuren er økende, og at mulighetsrommet av uønskede hendelser som kan ramme virksomheter, infrastrukturer og tjenester innenfor elektronisk kommunikasjon er stort. Bransjen og myndighetene må fortsatt rette oppmerksomhet mot fordekte operasjoner som har til hensikt å påvirke (eller etablere evne til å påvirke) nett og -tjenesters integritet og konfidensialitet.*

- *Sårbarheter – høy fart i digitaliseringen av samfunnet medfører nye sårbarheter. I årets rapport setter Nkom søkelys på økende kompleksitet i verdikjeder og sårbarheter som følger av selve overgangsperioden når ny teknologi og nye sikkerhetsløsninger blir innført og må samvirke med eldre teknologi.*

Utbyggingen av 5G gir fantastiske teknologiske muligheter, også innenfor sikkerhet. Den vil imidlertid også bringe med seg en del kjente utfordringer ved rask teknologiutvikling, slik som sårbarheter og avhengigheter i sameksistens mellom ny og gammel teknologi og tilgang på kompetanse.

Den digitale grunnmurens motstandsdyktighet og tilpasningsevne blir avgjørende for ekomsikkerheten fremover. I EkomROS 2019 peker vi på tiltak for å bygge en digital grunnmur som er solid nok for både dagens og fremtidens Norge. Dette innebærer å bygge diversitet i systemene, etablere responsevne til å avdekke og håndtere digitale angrep, ha beredskap til å håndtere uforutsette hendelser og ikke minst å sørge for høy sikkerhetskompetanse i organisasjonene.

INNHOLD

1

INNLEDNING

Virksomheter som tilbyr elektroniske kommunikasjonsnett eller -tjenester (ekom) i det norske markedet, er pålagt å utarbeide beredskapsplaner og tiltak for å opprettholde forsvarlig sikkerhet i sine ekomnett og -tjenester. Som bakgrunn for slike planer og tiltak skal det gjøres risiko- og sårbarhetsanalyser (ROS). Vurderingene skal ta utgangspunkt i egen virksomhet, tjenesteproduksjon og den infrastruktur de bruker.

Gjennom det løpende forvaltningsarbeidet, tilsynsarbeid og samarbeidet med sektoren, får Nkom oversikt over de ulike tilbydernes og aktørenes nett- og tjenester, og deres utviklingsplaner. Nkom mottar mange varsler om konkrete sikkerhetshendelser i ekomnettene. Nkom EkomCERT innhenter og sammenfatter informasjon om sårbarheter, trusler og hendelser i det digitale domenet. Til sammen danner disse informasjonselementene et viktig fundament for Nkoms risikovurderinger.

Nkom har utstrakt samarbeid både med andre sektormyndigheter og regionale myndigheter, og er også en del av totalforsvaret.

Nkom gir ut EkomROS for fjerde året på rad.

[1] *Nkom EkomCERT er ekomsektorens responsmiljø for informasjonsdeling, koordinering og varsling ved logiske sikkerhetshendelser i sektoren.*

2

EkomROS 2016 – 2018

I rapportene fra 2016, 2017 og 2018 har Nkom beskrevet totalt ni utviklingstrekk og elleve risikoområder for ekomsektoren. Utviklingstrekkene har vist seg å være treffende for utviklingen i sektoren og de fleste gjelder fortsatt. De identifiserte utviklingstrekkene og risikoområdene er oppsummert i figur 1.

UTVIKLINGSSTREKK		
2016	**2017**	**2018**
• *Samfunnsavhengighet og Totalforsvaret* • *Fra fysiske til logiske nettverk* • *Utkontraktering og internasjonalisering*	• *Mobilnettene bærer samfunnet på sine skuldre* • *Veien mot 5G, virtualisering og automatisering* • *Markeds- og aktørbilde i endring - nye konstellasjoner*	• *Fremtidens nød- og beredskapstjenester i kommersielle mobilnett* • *Nye muligheter og utfordringer med 5G og IoT* • *Tilstrekkelig kompetanse i egen organisasjon*
RISIKOOMRÅDER		
2016	**2017**	**2018**
• *Nasjonal sambands-infrastruktur og sentralisering av tjenesteproduksjon* • *Kompleks verdikjede og omfattende utstyrsporteføljе* • *Utkontraktering og inter-nasjonalisering*	• *Minsket nasjonal kontroll på kritisk tjenesteproduksjon* • *Hybride trusler - økt fare for integritets- og konfidensialitetsbrudd* • *Forstyrrelser i kritisk trådløs kommunikasjon* • *Sårbar infrastruktur i nordområdene*	• *Økt avhengighet til satellittnavigasjonstjenester* • *Ekomsektorens betydning for totalforsvaret* • *Nødnett i kommersielle nett* • *Økt omfang av IoT*

Figur 1 – oversikt over identifiserte utviklingstrekk og risikoområder fra Nkoms rapporter «EkomROS» fra 2016 til 2018.

Nkom har beskrevet samfunnsmessige, teknologiske og organisatoriske utviklingstrekk som på ulike vis har påvirket utviklingen i ekomsektoren og hvordan ekomsektoren har hatt betydning for samfunnet for øvrig.

Samfunnsmessige utviklingstrekk

I det samfunnsmessige perspektivet har Nkom beskrevet hvordan stadig flere kritiske samfunnsfunksjoner bæres av elektroniske kommunikasjonsnett og -tjenester. Nkom har blant annet pekt på Forsvarets kommunikasjonsbehov som i økende grad må dekkes av sivile tjenester, og at fremtidens nødnett skal bygges i de kommersielle mobilnettene.

Teknologiske utviklingstrekk

Nkoms beskrivelse av de teknologiske utviklingstrekkene startet med overgang fra fysiske til logiske nettverk. Nkom har blant annet beskrevet hvordan produksjon av ekomtjenester som tidligere bestod av spesialiserte produkter av maskin- og programvare på separate infrastrukturer, i økende grad blir realisert på felles IP-basert infrastruktur og gjennom konfigurerbar programvare på standardiserte komponenter.

I 2016 og 2017 skjøt interessen rundt 5G fart, og utviklingstrekk og sårbarheter tilknyttet denne utviklingen ble beskrevet.

Massiv økning av IoT, økende kompleksitet og kunstig intelligens har blitt trukket frem som resultat av ny teknologi.

I 2018 uttrykte Nkom bekymring for at mye av IoT-utstyret som vil komme på markedet kan ha for dårlig innebygd sikkerhet, og at dette kan utnyttes til å gjennomføre tjenestenektangrep.

Organisatoriske utviklingstrekk

I beskrivelsen av organisatoriske utviklingstrekk, ble det først rettet fokus mot utkontraktering og internasjonalisering. Nkom påpekte at tjenesteutsetting kan ha mange fordeler, men at det samtidig innebærer en ytterligere fragmentering av tilbyders ansvar og oppgaver som kan utfordre både sikkerheten i nett og personvern.

I 2016 og 2017 ble det satt søkelys på stadig økende avhengighet av utstyrsleverandører og andre underleverandører av tjenester, og endringer i markeds- og aktørbildet. Eksempel på dette er de store internettaktørene som tilbyr tale- og meldingstjenester *over-the-top (OTT)*, som iMessage, Skype, Whatsapp osv. I 2018 ble det vist til behovet for å sørge for tilstrekkelig kompetanse i organisasjonene.

EkomROS 2016, 2017 og 2018 er tilgjengelige på nkom.no.

3

ERFARINGER FRA 2018

3.1 Oversikt over større hendelser

Ekomtilbyderne plikter å varsle Nkom om hendelser som vesentlig kan redusere eller har redusert tilgjengeligheten til elektroniske kommunikasjonsnett og -tjenester. Nkom har døgnvakt som mottar informasjon fra ekomaktørene om hendelser og utfall. Ut fra hendelsens omfang og alvorlighetsgrad, vil Nkom undersøke årsakssammenhengene og vurdere tiltak.

Oversikten tar utgangspunkt i hendelser av en viss alvorlighetsgrad som er registrert og fulgt opp av Nkom i 2018. Datagrunnlaget gir oversikt over antall registrerte hendelser, tidspunkt for hendelsen, type feil og hendelsens alvorlighetsgrad.

Antall hendelser og alvorlighetsgrad

I 2018 ble det registrert 61 hendelser med større lokale eller regionale utfall som hadde en alvorlighetsgrad som medførte oppfølging fra Nkom. Erfaringene fra 2018 er omtrent som tidligere år.

Alvorlighetsgraden ved uønskede hendelser er knyttet til beredskapsnivå. Oversikten i figur 2 beskriver Nkoms beredskapsnivå.

I 2018 ble 18 hendelser registrert som NORMAL, 42 hendelser som GRØNN og én hendelse som GUL. Ingen hendelser ble registrert som ORANSJE eller RØD.

GRØNN:	Økt beredskap, enkeltfunksjoner og ressurser kan forsterkes.
GUL:	Begrenset mobilisering av ekstra ressurser.
ORANSJE:	Mobilisering av større ressurser og omlegging av drift i én avdeling.
RØD:	Mobilisering av betydelige ressurser og omlegging av drift i to eller flere avdelinger.

Figur 2 – Nkoms beredskapsnivå

Hendelser per kategori

Hendelsene som er registrert hos Nkom er inndelt i kategorier ut fra type feil eller årsak.

Figur 3 viser hendelser fordelt på kategori. Som for tidligere år utgjorde fiberbrudd og programvarefeil de vanligste årsakene til utfall i 2018, der omtrent halvparten var direkte knyttet til fiberbrudd. Programvarefeil stod bak omtrent en fjerdedel av utfallene. Ekstremvær og tap av ekstern kraft var også viktige feilårsaker.

To av hendelsene er kategorisert som GNSS[2] -forstyrrelser, det vil si frekvensforstyrrelser som rammer systemer for satellittnavigasjon. Slike frekvensforstyrrelser kan være tilsiktet ved bruk av jammeutstyr, eller utilsiktet som følge av for eksempel tekniske feil i radiosendere eller utstyr som ikke er godkjent for bruk i Norge.

Nkom har observert flere tilfeller av GNSS-forstyrrelser i 2018 enn de to hendelsene som fremkommer av oversikten. Disse to utpekte seg imidlertid som spesielt alvorlige. Begge hendelsene gjaldt problemer ved flyplasser i Finnmark.

[2] *Global Navigation Satellitte System, for eksempel GPS.*

Hendelser per måned

Fiberbrudd og programvarefeil er relativt jevnt fordelt over hele året. Selv om fiberbrudd oftere forårsaker utfall, får programvarefeil potensielt større konsekvenser. Fiberbrudd leder som oftest til lokale og i noen tilfeller regionale utfall. Programvarefeil oppstår gjerne i forbindelse med oppdateringer eller endringer i sentrale komponenter i infrastrukturen, og kan få store konsekvenser som kan ramme nett og tjenester i hele landet.

Utfall knyttet til ekstremvær skjer hovedsakelig om høsten og vinteren. Større utfall knyttet til tap av ekstern kraft inntreffer hovedsakelig om vinteren. Med stadig mer ekstremvær kan dette endre seg.

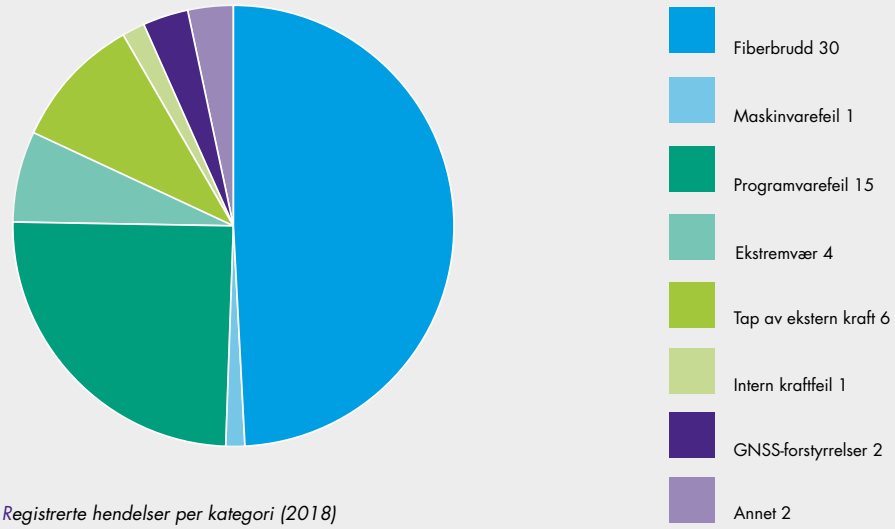
To hendelser er kategorisert under «annet». Hendelsen i februar var knyttet til økt beredskap på grunn av en tilbyders flytting av en kritisk kjernenettkomponent fra utlandet til Norge (ingen feil oppsto). Hendelsen i november omhandlet anmoding fra Hovedredningssentralen om bistand i forbindelse med søk etter et savnet fly.

Oktober og november 2018 har flest registrerte hendelser. I denne perioden var det registrert flere typer feil og utfall som sammenfaller i tid. Hendelsene omhandlet hovedsakelig fiberbrudd, programvarefeil og tap av ekstern kraft.

Kategori utfall	Forklaring
Fiberbrudd	*Brudd på fiberoptiske kabler på land eller i sjø, for eksempel brudd etter gravearbeid eller på grunn av slitasje*
Maskinvarefeil	*Fysiske feil i kritiske komponenter, for eksempel feil i nettverkskort eller fysiske skader eller feilkoblinger i forbindelse med planlagt arbeid*
Programvarefeil	*Logiske feil i kritisk programvare, for eksempel feil i brannmurer, feil i forbindelse med programvareoppdateringer eller endringer i databaser, eller andre former for feilkonfigurering*
*Ekstremvær**	*Ekstremvær, som ekstrem nedbør eller storm*
Tap av ekstern kraft	*Svikt i ekstern kraftforsyning, for eksempel strøm til basestasjoner*
Intern kraftfeil	*Interne feil i kraftforsyningen, for eksempel svikt i batteribanker, aggregater eller tavler*
GNSS-forstyrrelser	*Utilsiktede eller tilsiktede frekvensforstyrrelser som rammer satellittnavigasjonssystemer*
Annet	*Samlebetegnelse for uønskede hendelser som ikke faller inn under de øvrige kategoriene*

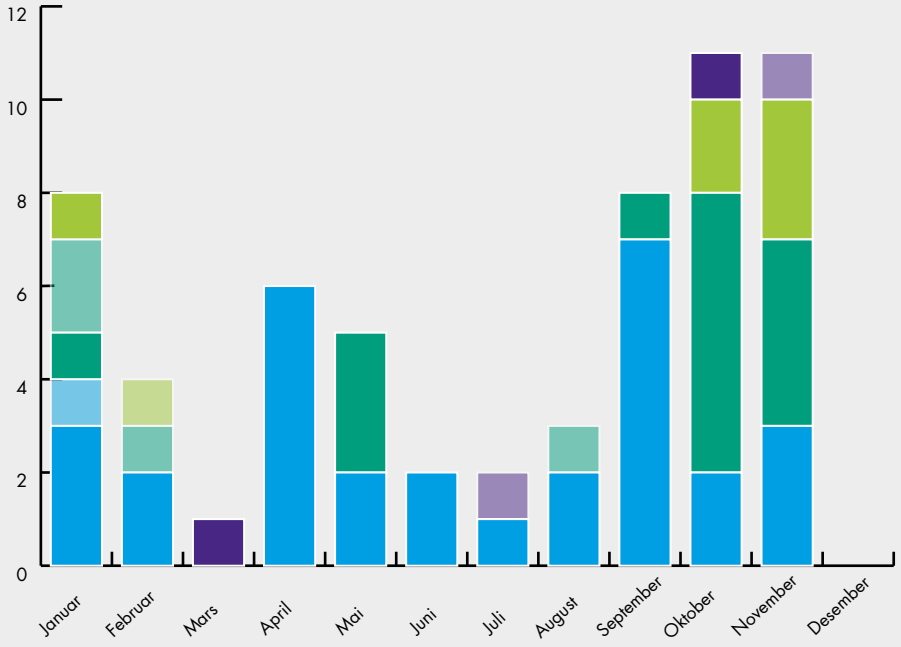
** Utfall hvor rotårsaken er ekstremvær. Det utelukker ikke at f.eks. fiberbrudd eller strømbrudd inngår i kjeden av årsaker, men utfall er i de tilfellene registrert på rotårsaken, ekstremvær*

REGISTRERTE HENDELSER PER KATEGORI (2018)



Figur 3 - Registrerte hendelser per kategori (2018)

ANTALL HENDELSER PER MÅNED OG KATEGORI (2018)



Figur 4 - Antall hendelser per måned og kategori (2018)

Hendelser rapportert til ENISA

EUs byrå for nettverks- og informasjonssikkerhet (European Union Agency for Network and Information Security - ENISA) har som hovedformål å styrke nettverks- og informasjonssikkerheten i EU. Norge er tilknyttet ENISA og har observatørstatus i ENISAs styre. Nkom deltar i flere arbeidsgrupper i regi av ENISA, blant annet med oppgaver knyttet til hendelsesrapportering og tillitstjenester.

Enkelte hendelser i EU/EFTA-landene, med betydning for nettverks- og informasjonssikkerhet, blir rutinemessig rapportert videre til ENISA, og blir inkludert i byråets Annual Incident Report.

Nkom rapporterer hendelser som er av nasjonal betydning til ENISA. I 2018 har Nkom rapportert følgende tre hendelser:

Fiberbrudd og feil i forbindelse med planlagt arbeid

I november 2018 opplevde flere kommuner i Øst-Finnmark samtidig utfall på fasttelefoni, bredbånd og mobil tale, data og meldingstjenester. I tillegg ble Nødnett og Kystradioen rammet. Utfallet var forårsaket av to feil som sammenfalt i tid, og varte i omtrent seks timer. Dermed mistet store deler av Øst-Finnmark tilgang til nett og tjenester.

Programvarefeil i brannmur og signaleringsstorm

I oktober 2018 oppstod et stort utfall på mobil tale, data og meldingstjenester som følge av en programvarefeil hos et mobilselskap.
Feilen rammet kunder i hele landet. Da feilen var rettet og kundene skulle kobles til på nytt, forårsaket dette en signaleringsstorm som førte til overbelastning i mobilselskapets mobilnett. Selve programvarefeilen ble rettet i løpet av én time. Signaleringsstormen medførte ustabilitet i rundt fem timer.

Uautorisert endring i kjernenettet

I april 2018 opplevde en aktør et stort utfall på tale- og meldingstjenester som følge av en uautorisert endring i programvare. Feilen skyldtes en endring i sentral infrastruktur og medførte utfall i tilbyderens tjenester i hele landet. Feilen ble rettet etter kort tid ved å reversere endringen, og tjenestene var stabile igjen etter rundt tre timer.

Hendelser i andre europeiske land

ENISAs årlige hendelsesrapport for ekomsektoren gir en oversikt over de store trendene i Europa. Uønskede hendelser er her delt inn i fire rotårsaker: systemfeil, menneskelige feil, naturfenomener og tilsiktede hendelser. Systemfeil i denne sammenhengen kan være feil knyttet til både maskinvare og programvare, ofte i sammenheng med endringer eller oppdateringer. Menneskelige feil dekker utfall som er en konsekvens av at rutiner og prosedyrer ikke er fulgt. Naturfenomener dreier seg om vær og vind, mens tilsiktede hendelser kan gjelde både cyberangrep og fysisk ødeleggelse.

Antall hendelser som rapporteres til ENISA har holdt seg nokså jevnt år for år, med en variasjon på mellom 130 og 170 hendelser for Europa totalt. Opptil 70 prosent av utfallene knyttes til feil i maskinvare eller programvare. Systemfeil er som regel årsaken til de største utfallene. Det samme erfarer vi i Norge, der programvare- eller maskinvarefeil i sentrale deler av infrastrukturen potensielt rammer nett og tjenester i hele landet.

I ENISAs hendelsesrapport for 2018 er naturfenomener for første gang oppgitt som årsaken til utfallene med flest tapte brukertimer. Dette er primært knyttet til mange strømbrudd som medførte store konsekvenser for brukerne. Tilsiktede hendelser hadde færrest antall tapte brukertimer.

3.2 Cybertrusler

Nkoms responsmiljø Nkom EkomCERT overvåker en jevn strøm av cybersikkerhetstrusler som kan ramme ekomsektoren. Vi vil særlig trekke frem to eksempler på trusler som har fått oppmerksomhet internasjonalt den siste tiden.

DNS-kapring

Domain Name System (DNS) er en tjeneste som er helt nødvendig for at Internett skal fungere. DNS knytter domenenavn til IP-adresser og bidrar til at trafikk på Internett sendes til riktig sted. De siste årene har vi sett en økning i antall sikkerhetshendelser der angripere utnytter sårbarheter i DNS for å ta kontroll over trafikk inn og ut av målets kjernekomponenter, gjerne som et ledd i et «*man-in-the-middle*»-angrep.

I løpet av 2018 har vi sett flere tilfeller av DNS-kapring. Angrepene utnyttet administrative tilganger hos forhandlere av domenenavn (registrarer) for å endre oppføringene av autorative DNS-servere. Ved å kontrollere DNS-oppføringene kunne angriperne bestille nye krypteringssertifikater og plassere seg som et mellomledd for systemer som for eksempel e-post, og på denne måten hente ut informasjon som brukernavn og passord. Angrepene var rettet mot mål i Nord-Amerika, Europa, Nord-Afrika og Midtøsten.

Utnyttelse av sårbarheter i kundenes utstyr

Rutere og annet kundeplassert utstyr er sårbar for angrep dersom det ikke blir oppdatert. Mange kunder er opptatt av å sikre at PC og mobiltelefon har de nyeste oppdateringene, men glemmer at annet nettverksutstyr, som for eksempel hjemmeruteren, også må oppdateres og sikres. Det at nettverksutstyr ikke blir oppdatert kan også skyldes mangel på automatisk oppdatering. Enheter som ikke er oppdatert er en potensiell inngangsport for blant annet skadelig programvare.

VPNFilter er et eksempel på en skadelig programvare med stort skadepotensial. Her utnyttes kjente sårbarheter i kundeplassert nettverksutstyr hos små- og mellomstore bedrifter og i privatmarkedet. VPNFilter benyttes til informasjonsinnsamling og destruktive angrep. Programvaren utnytter også utstyr der standardpassord fra leverandør ikke er endret av brukeren. Våren 2018 ble VPN Filter benyttet til å infiltrerte omtrent 500 000 enheter i mer enn 54 land. VPNFilter har en del likhetstrekk med BlackEnergy, som ble benyttet i angrep rettet mot energiforsyningen i Ukraina i 2015.

3.3 GNSS-forstyrrelser

Global Navigation Satellite System (GNSS) er fellesbetegnelsen på satellittbaserte systemer for navigasjon, posisjonering og tidsangivelse. Det amerikanske GPS og det russiske GLONASS har vært etablert i lang tid, mens europeiske Galileo og kinesiske BeiDou fortsatt er under oppbygging. Bruken av GNSS-enheter er omfattende og øker stadig, ikke minst på grunn av GNSS-enheter installert i personlig utstyr som telefoner og klokker.

GNSS-signalene kommer fra satellitter og er svake og dermed sårbare for forstyrrelser. Signalene kan hovedsakelig forstyrres på to måter: jamming og spoofing. Å jamme betyr å sende støysignaler i det aktuelle frekvensområdet for å forstyrre mottaket av signaler. Spoofing går ut på å sende falske GNSS-signaler som manipulerer tidsinformasjon og posisjon, og kan utgjøre en alvorlig trussel for lufttrafikk.

Nkom har observert flere tilfeller av omfattende GNSS-forstyrrelser i 2018 og hittil i 2019, både i Nord-Norge og Sør-Norge. Forstyrrelser har spesielt rammet luftfarten som er helt avhengig av navigasjonssystemer som benytter GNSS-signaler.

Støysignaler rammer lufttrafikken

Flere steder i landet er det påvist privateide jammere som har skapt forstyrrelser, blant annet for Norsk Luftambulanse. Slikt utstyr blir gjerne brukt av personer som ønsker å skjule egen posisjon, for eksempel sjåfører som bruker arbeidsgivers kjøretøy og vil unngå sporing. Støysignalene som sendes ut kan påvirke GNSS-signalene i større områder opp til flere kilometer fra senderen. Slikt jammerutstyr er ulovlig i Norge.

I mars 2018 ble det rapportert om forstyrrelser av GPS-signalene i luftrommet over Øst-Finnmark. Observasjonene liknet på hendelser i 2017. Under NATO-øvelsen Trident Juncture i oktober og november 2018, ble det igjen observert signalforstyrrelser i Nord-Norge. Årsaken var på dette tidspunktet ukjent og i samråd med Forsvaret og andre etater ble det besluttet at Nkom på det daværende tidspunkt ikke skulle utføre nye målinger. I sin åpne og ugraderte årlige trussel- og risikovurdering, Fokus 2019, knytter Etterretningstjenesten disse tilfellene til aktivitet på russisk side av grensen.

GNSS-forstyrrelsene har fortsatt i 2019. I slutten av februar utførte Nkom nye målinger i Bodø og Tromsø som følge av ny varsling fra Luftfartstilsynet om signalforstyrrelser i Nord-Norge. Så langt i 2019 har Nkom vært involvert ved flere hendelser der luftambulansen har vært rammet av støysignaler. Disse hendelsene knyttes hovedsakelig til ulovlig jammerutstyr i kjøretøy.

Ny målestasjon i Finnmark

På grunn av gjentatte tilfeller av GNSS-forstyrrelser i Finnmark, har Nkom besluttet å opprette en fjernstyrt målestasjon i Sør-Varanger. Målestasjonen kan registrere hvor støysignaler kommer fra. Dataene fra disse målestasjonene brukes til analyser av uønsket frekvensbruk. Målestasjonen ble satt i drift første halvår i 2019. I tillegg har Nkom et titalls slike målestasjoner rundt omkring i landet, hovedsakelig i tett befolkede områder.

3.4 Mobilkapring

De fleste har knyttet sitt telefonnummer opp mot ulike tjenester på Internett, blant annet kontoer i sosiale medier, e-post og strømmetjenester. Telefonnummeret benyttes gjerne også som nøkkel til gjenoppretting av tilgangen dersom man blir låst ute av en tjeneste, for eksempel der man har glemt passordet. Dette gjør telefonnummeret til et mål for identitetstyveri.

Problemstillingen ble belyst i en serie oppslag i media i mars 2019. Porteringssvindel går ut på at uvedkommende bestiller overføring av et eksisterende telefonnummer til et annen mobil-selskap. Uautorisert endring av SIM-kort går ut på at uvedkommende endrer SIM-kortet som er knyttet til et telefonnummer, enten ved å bestille et nytt SIM-kort i kundens navn eller ved å overføre telefonnummeret til et SIM-kort svindleren allerede besitter. Begge metodene fører til at kunden mister kontrollen over eget telefonnummer, og svindleren kan benytte seg av dette for å få tilgang til tjenester og opplysninger.

For å portere et nummer eller bestille endring av SIM-kort, må svindleren gå gjennom et mobilselskap. Nkom stiller derfor en rekke krav til håndteringen av slike bestillinger. Selskapet skal sikre entydig og rett identifisering av kunden, før overføringen blir gjennomført. Det er gjerne identitetskontrollen som er det svake leddet.

Det er viktig å ivareta prinsippet om at det skal være enkelt for kunden å bytte mobilselskap (portere). Derfor er enkle rutiner for å overføre et telefonnummer mellom selskaper, essensielt for kundens valgfrihet og konkurranse i markedet. Fordi telefonnummeret er


Alexandria Ocasio-Cortez: Sjokkerte USA med klima-forslag - fikk uventet støtte

DN Dagens Næringsliv

SAS planlegger for fremtidens flyreiser

Da vil du ikke møte en person her du er om bord på flyet, ifølge SAS-sjef Rickard Gustafson.

Eva Grinde: Solskjær-dyrkingen viser hvilken enorm makt vi tillegger fotballsjefer

Søvnmangel bie vekker for toppsjef → S.18 Gamingsuksess ga gigantbonus → S.16

Digitaliseringsminister Nikolai Astrup om mobilkapring:

– Rystende å lese

Nasjonal kommunikasjonsmyndighet vil komme til bunns i hva som skjedde da DN fikk overta andre personers mobilnumre uten gyldig ID. → S.4–7

Faksimile: Dagens Næringsliv, 11. mars 2019

og betydelige mengder informasjon om brukeren, er det imidlertid også viktig å vurdere hvordan svakheter i porteringsprosesser kan utbedres. Derfor vurderer Nkom ytterligere krav til sikker identifisering av kunden ved portering.

4

UTVIKLINGSTREKK FREMOVER

4.1 Det generelle trusselbildet

I utarbeidelsen av EkomROS henter Nkom informasjon om ekomsektoren gjennom tilsynsvirksomhet, dialog med tilbydere av ekomtjenester, oppfølging av konkrete hendelser og fra samarbeid med relevante aktører. De årlige trussel- og risikovurderingene fra Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) er også viktige kilder i Nkoms sikkerhetsarbeid. Vi bruker også Direktoratet for samfunnssikkerhet og beredskap (DSB) sine analyser av krisescenarioer for å identifisere samfunnskonsekvenser som følge av sikkerhetshendelser i ekomsektoren.

NSM: «Risiko 2019»

Ekom er avhengig av kraft. I rapporten «Risiko 2019» viser imidlertid NSM til at all infrastruktur, inkludert kraft, også blir mer og mer avhengig av elektronisk kommunikasjon. NSM sier også at 5G vil danne grunnlaget for nye tjenester og funksjoner og skape ytterligere avhengigheter. Av trusler som Norge står overfor, er særlig fremmed etterretning, nettverksoperasjoner, andre digitale trusler, påvirkningsoperasjoner, innsidere, strategiske investeringer og oppkjøp, kartlegging, jamming og terror viktig å være oppmerksom på, nærmest uansett bransje.[3]

NSM har identifisert seks risikofaktorer som må håndteres de kommende årene:

- *Et ufullstendig risikobilde*
- *Svak sikkerhetsstyring*
- *Svakheter eller mangler i virksomhetens personellsikkerhetsarbeid*
- *Utilstrekkelig sikring av samfunnsviktig informasjon og informasjonssystemer*
- *Manglende kartlegging av avhengigheter og dermed manglende helhetlig sikring av objekter og infrastrukturer*
- *Et næringsliv som i enda større grad vil levere tjenester og utstyr til viktige samfunnsfunksjoner i fremtiden* [4]

Disse risikofaktorene vil også være relevant å vurdere i sammenheng med sikkerhetsarbeidet i ekomsektoren.

PST: «Trusselvurdering 2019»

PST kategoriserer trusler slik: statlig etterretningsvirksomhet, politisk motivert vold og trusler mot myndighetspersoner. PST vurderer det som sannsynlig at utenlandske etterretningstjenester vil forsøke å påvirke beslutninger til private og offentlige aktører, og trekker frem statlig styrte nettverksoperasjoner som en vedvarende trussel mot norske verdier. PST sier at metodene som brukes er billige, effektive og i konstant utvikling, og angripere finner stadig nye sårbarheter de kan utnytte.[5]

E-tjenesten: «Fokus 2019»

Som PST, omtaler E-tjenesten etterretningstrusselen som en pågående og omfattende sikkerhetsutfordring mot Norge og norske interesser de neste årene, og at trusselen er størst fra Russland og Kina. E-tjenesten skriv-

3 «Risiko 2019 – Krafttak for et sikrere Norge.» NSM rapport 2019
4 «Risiko 2019 – Krafttak for et sikrere Norge.» NSM rapport 2019
5 «Trusselvurdering 2019.» PST rapport 2019

er at nettverksoperasjonene blant annet har vært rettet mot norske styresmakter og kommersielle selskaper innenfor flere sektorer. I tillegg forventer de at russiske påvirkningsforsøk med mål om å undergrave politiske prosesser og øke polariseringen i Europa og NATO, vil fortsette. E-tjenesten legger også vekt på at det militære samarbeidet mellom Russland og Kina vokser og at vi på sikt må være forberedt på et tydeligere kinesisk nærvær også i våre nærområder.[6]

I likhet med NSM, peker E-tjenesten på «jamming» som en trussel som gir særlig grunn til bekymring. Begge trekker frem erfaringene fra NATO-øvelsen Trident Juncture 2018, som også er beskrevet i kapittel 3 i denne rapporten. E-tjenesten viser i tillegg til den teknologiske utviklingen som et viktig moment i utviklingen av trusselbildet:

> *«Den teknologiske utviklingen har ført til at handlingsrommet til både statlige og ikke-statlige aktører har vokst. Denne utviklingen vil fortsette. Stadig flere både statlige og andre aktører vil få tilgang til avanserte våpensystemer og produksjonskapasiteter. Det vil forsterke trenden mot et sektoroverskridende trusselbilde.»*
>
> Fokus, E-tjenesten 2019

ENISA: «ENISA Threat Landscape 2018»

ENISA-rapporten [7] presenterer en oversikt over de mest aktuelle truslene innenfor cyberdomenet fra 2018. Rapporten omtaler hva som kalles hele økosystemet for trusler mot cybersikkerhet, og viser samtidig en oversikt over de 15 mest aktuelle truslene fra året før. I rapporten for 2018 er skadelig programvare («Malware») rangert som den største trusselen, internettbaserte angrep («Web Based Attacks») kommer som nummer to og angrep mot internettapplikasjoner («Web Application Attacks») som nummer tre. I årets rapport trekker de også frem begrepet «Cryptojacking», som brukes om å utnytte andres datamaskiner for å høste gevinst fra kryptovaluta.

Klimaendringer

FNs klimapanel har slått fast at at verden siden førindustriell tid har blitt omtrent 0,8 grader varmere. Selv om de fattigste landene er mest utsatt for konsekvenser av klimaendringene, vil også Norge bli rammet. I Norge har nedbøren økt med om lag 20 prosent de siste hundre årene, og har samtidig blitt mer intens. Risikoen for flom øker.[8] I «Analyser av krisescenarioer 2019» har DSB samlet 25 risikoanalyser av alvorlige hendelser som kan ramme det norske samfunnet. Ett av scenarioene er «Regnflom i by», hvor blant annet ustabile elektroniske kommunikasjonsløsninger trekkes frem som en utfordring for samfunnsstabiliteten.[9]

4.2 Digitalisering

Digitalisering av samfunnet, ofte omtalt som den fjerde industrielle revolusjon, har for lengst startet. Stortingsmeldingen Digital agenda[10] beskriver blant annet betydningen av IKT for å forbedre offentlig sektor og legge til rette for innovasjon og konkurransekraft i næringslivet.

Meldingen presenterer også en nasjonal plan for elektronisk kommunikasjon. Planen beskriver behovet for en offensiv ekompolitikk for å sikre oppgraderinger og nyinvesteringer i ekomnett. Dette er viktig for å kunne tilby

---

6 «Fokus 2019 – Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.» E-tjenesten rapport 2019
7 «ENISA Threat Landscape 2018.» ENISA report 2019
8 Kilde: https://www.regjeringen.no/no/tema/klima-og-miljo/klima/innsiktsartikler-klima/klimaendringer/id2076641/
9 «Analyser av krisescenarioer 2019», DSB rapport 2019
10 Meld. St. 27 (2015-2016) Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet

nye tjenester. Ny regjeringsplattform (Granavoldplattformen) fastslår at digitaliseringsarbeidet skal fortsette i tråd med føringene fra Digital agenda, men også at arbeidet med innovasjon i offentlig sektor må forsterkes for å sikre gode tjenester, bedre samordning og god bruk av samfunnets ressurser [11].

Av DESI (The Digital Economy and Society Index) – indeksen går det frem at Norge allerede er et av verdens mest digitaliserte samfunn. I 2018 ble Norge rangert som nummer fem i Europa, like bak de andre skandinaviske landene[12] I indeksen måles landene blant annet på digital infrastruktur, teknologikompetanse, og bruk av teknologi og internett-tjenester i samfunnet. Norge har ifølge indeksen særlig fremgang på områdene «bruk av IKT i næringslivet» og «offentlige digitale tjenester».[13] NHOs perspektivmelding fra 2018, «Verden og oss»,[14] omtaler digitalisering i et eget kapittel:

> *«Norge har et godt utgangspunkt. Vi har en velfungerende digital infrastruktur, et kompetansebasert næringsliv og sterke næringer med internasjonalt nedslagsfelt. Vi har en offensiv offentlig sektor som tar i bruk nye digitale tjenester, og en velutdannet befolkning som tidlig tar i bruk nye teknologier.»*
>
> «Verden og oss»,
> Næringslivets hovedorganisasjon (NHO) 2018

Teknologikompetanse

DESI-Indeksen viser samtidig at Norge siden 2017 har hatt liten eller ingen fremgang på teknologikompetanse. Andelen uteksaminerte innen matematikk, naturfag og teknologifag er redusert og andelen IT-spesialister har ikke økt. I EkomROS 2018 rettet Nkom oppmerksomhet mot det økende behovet for kompetanse i bransjen. Tilbydere av elektronisk kommunikasjon synes i stadig større grad å bli avhengig av utstyrsleverandører og andre underleverandører av tjenester. Dette skyldes både behov for spesialkompetanse og for kostnadseffektivisering. Jo lengre og mer kompleks leverandørkjeden er, dess mer krevende vil det bli å opprettholde forsvarlig kontroll med for eksempel sikkerhet i nett og tjenester. Sikring av kritisk kompetanse vil derfor bli svært viktig i tiden fremover.

Digital tillit

Det er ikke gitt at alle brukere tar i bruk ny og tilgjengelig teknologi, selv om den er tilgjengelig. En viktig forutsetning for å sikre stadig fremgang, er tilliten til tjenestene som blir tilbudt og brukt i hverdagen. Digital tillit er nøkkelen til økt bruk av nye digitale tjenester og gjenspeiles i at brukerne opplever tjenester som brukervennlige og sikre. Det vil med andre ord være kritisk at tjenester og funksjoner som tilbys har tilstrekkelig integritet, konfidensialitet og tilgjengelighet, i tillegg til at de må de være brukervennlige.

Den økte digitaliseringen gjør at virksomheter kan samle inn store mengder data om brukerne, selv om lovgivningen på området er skjerpet med innføringen av GDPR («General Data Protection Regulation») i Europa i 2018. Nye IoT-tjenester og utstyr vil også bidra til at ny type informasjon blir samlet inn og at informasjonen blir brukt på måter som er vanskelig å kunne forutse. Den store mengden informasjon kan sammenfattes og brukes til å forenkle hverdagen til mennesker og virksomheter. Dette krever imidlertid at data som samles inn er korrekte og at brukerne faktisk benytter seg av de nye tjenestene,

11 Kilde: https://www.regjeringen.no/no/dokumenter/politisk-plattform/id2626036/
12 Digital Economy and Society Index (DESI) 2018 Country Report Norway-https://www.regjeringen.no/contentassets/5d2caddad8424250846b8dc93e259997/desi-indeksen_2018_norge.pdf
13 Kilde: https://www.regjeringen.no/no/aktuelt/fortsatt-blant-de-ledende-landene-i-europa-pa-digitalisering/id2601593/
14 Kilde: https://www.nho.no/publikasjoner/p/naringslivets-perspektivmelding/

i trygg forvissing om at personopplysninger eller andre data ikke blir misbrukt eller gjort tilgjengelige for uvedkommende.

Norge har gode løsninger som ivaretar informasjonssikkerheten i offentlige tjenester. Dette er viktig for digitalisering av samfunnet. BankID er et eksempel på en tillitstjeneste, som består av kontroll- og valideringsmekanismer som skal sikre autentisitet ved bruk av tjenesten. Nkom er tilsynsmyndighet for tillitstjenester. En ny lov om tillitstjenester trådte i kraft 15. juni 2018. Denne skal bidra til økt elektronisk samhandling mellom næringsdrivende, innbyggere og offentlige myndigheter på tvers av landegrensene i EØS-området. Regelverket legger til rette for sikrere elektronisk samhandling på nett, og målet er økt tillit fra forbrukerne.[15]

Store forventninger til 5G og IoT

Forventningene til 5G-teknologi er store og utbredelsen av 5G og Internet of Things (IoT) vil stå sentralt i den videre digitaliseringen av samfunnet. Utviklingspotensialet er stort og legger til rette for nye bruksområder i flere bransjer og sektorer. Under et uformelt nordisk statsministermøte [16] i mai 2018 ble en intensjonserklæring om utviklingen av 5G i Norden signert. Erklæringen uttrykker felles mål om å bli den første og mest integrerte 5G-regionen i verden:

> *"As the development of fifth generation wireless systems (5G) breaks through, the Nordic countries will be at the forefront of that development to become world leaders in using 5G technology for the development and digitalisation of all sectors of society."* [17]

5G skal tilby høyere hastighet, lavere forsinkelse, økt pålitelighet og større kapasitet. 5G skal kunne legge til rette for et mer fleksibelt nettverk, slik at kritiske applikasjoner som for eksempel selvkjørende biler og helsetjenester som fjernkirurgi vil få «hvert sitt» nettverk innenfor det samme nettet.

IoT vil gi grunnlag for store kostnadsbesparelser for samfunnet og en forenklet hverdag for innbyggerne. Vi må derfor forvente at stadig flere IoT-applikasjoner vil bære viktige samfunnsverdier og ha kritisk betydning for liv, helse og sikkerhet. 5G antas å bli svært viktig for utbredelsen av IoT, og både industrien og myndigheten legger ned et betydelig arbeid i å sikre at teknologi i 5G har standardiserte løsninger som er spesielt beregnet for bruk av IoT. Standardene er utarbeidet for å støtte et bredt spekter av applikasjoner med ulike krav til kapasitet, forsinkelse, sikkerhet og batteriforbruk. Samtidig vil IoT introdusere mange nye IKT-utfordringer for samfunnet. Mange av disse utfordringene faller inn under, eller ligger nært opp mot, Nkoms samfunnsoppdrag.

4.3 Nye rammebetingelser

Som følge av, og parallelt med den raske teknologiutviklingen, blir nytt regelverk utviklet både på nasjonalt og europeisk nivå. Fellestrekk ved den nye reguleringen er endrede og forsterkede krav til digital sikkerhet og personvern. Nye krav gjelder på tvers av samfunnssektorer, og det skjer en harmonisering av krav til de som tilbyr ekomtjenester, enten det er de tradisjonelle ekomtilbyderne som Telenor og Telia, eller internettaktører som Apple og Google.

---

15 Kilde: https://www.regjeringen.no/no/aktuelt/nye-eu-regler-gir-okt-tillit-pa-nett/id2558439/
16 Kilde: https://www.regjeringen.no/no/aktuelt/nordisk-uformelt-statsministermote/id2601911/
17 «Intensjonserklæring om utvikling av 5G i Norden» - https://www.regjeringen.no/contentassets/9e75d374b20841e880fe5fc6aa6079fc/letter-of-intent-5g.pdf

Ny sikkerhetslov

Ny lov om nasjonal sikkerhet (sikkerhetsloven) trådte i kraft 1. januar 2019. Sikkerhetsloven legger opp til at virksomheter som har vesentlig eller avgjørende betydning for å opprettholde grunnleggende nasjonale funksjoner, skal beskyttes mot uønskede hendelser som kan ramme nasjonale sikkerhetsinteresser. Lovens virkeområde er utvidet fra informasjon og objekter, til også å inkludere informasjonssystemer og infrastruktur.
I ekomsektoren kan dette medføre at flere virksomheter blir underlagt sikkerhetsloven.

Loven er utformet med tanke på rask digital utvikling og stadig nye trusler. Departementene er ansvarlige for det forebyggende sikkerhetsarbeidet innenfor sine ansvarsområder, og en sentral oppgave er å identifisere og holde oversikt over sektorens «grunnleggende nasjonale funksjoner» og virksomhetene som understøtter disse. Virksomhetene skal på sin side kartlegge egne avhengigheter, vurdere risiko og beskytte skjermingsverdige verdier. Arbeidet med ny sikkerhetslov vil bli en vesentlig oppgave for Nkom og sektoren fremover.

Nytt europeisk ekomregelverk

Nytt europeisk ekomregelverk – European Electronic Communications Code (EECC) - ble vedtatt i EU i desember 2018 og skal innføres i EU senest desember 2020. Direktivet skal innlemmes i EØS-avtalen og gjennomføres i nasjonal rett i Norge. Blant de viktigste endringene er en ny definisjon av ekomtjenester som legger opp til en mer ensartet regulering av funksjonelt sett like tjenester. Dette betyr at en rekke kommunikasjonstjenester som blir levert via Internett i større grad skal reguleres tilnærmet likt som tradisjonelle tale- og meldingstjenester levert av dagens ekomtilbydere.

Det er fortsatt et skille mellom nummerbaserte og nummeruavhengige tjenester, slik at myndighetene kan stille strengere krav til nummerbaserte tjenester. Den nye ekomreguleringen åpner likevel for en mer ensartet regulering av sikkerhet, konfidensialitet og brukerrettigheter.

NIS-direktivet

Det nye europeisk ekomregelverket EECC er samkjørt med annen regulering med betydning for ekomsektoren, herunder NIS-direktivet («The Directive on security of network and information systems»). NIS-direktivet legger opp til en ny lov om nettverks- og informasjonssikkerhet på nasjonalt nivå, der det overordnede formålet er å styrket IKT-sikkerhet på tvers av sektorer. Dette innebærer blant annet en nasjonal strategi for IKT-sikkerhet og aktiv koordinering på europeisk nivå for å sikre et felles minimumsnivå.

NIS-direktivet retter seg spesielt mot leverandører av samfunnsviktige og digitale tjenester, og skal sikre at det stilles krav til IKT-sikkerhet uavhengig av sektor.

Kommunikasjonsvern

EU arbeider nå med en ny europeisk kommunikasjonsvernforordning (ePrivacy). Forordningen er en særlov for ekomsektoren og regulerer behandlingen av personopplysninger som genereres ved bruk av elektronisk kommunikasjon. Den må sees i sammenheng med *General Data Protection Regulation (GDPR)* som er implementert i norsk rett som personopplysningsloven.

Cybersikkerhet og 5G

Nytt europeisk regelverk får også innvirkning på cybersikkerhet. EU vedtok i mars 2019 en ny cybersikkerhetsforordning som blant annet legger opp til et permanent og styrket mandat for ENISA, og innføring av en europeisk cybersikkerhetssertifisering. Under den nye reguleringen kan ENISA bistå medlemslandene operativt ved cybersikkerhetshendelser. ENISA får også ansvaret for å utvikle et rammeverk for sikkerhetssertifisering av IT-produkter og -tjenester. Hensikten er økt transparens og verifisering, og dermed bidra til å realisere det digitale indre marked.

I en rekke europeiske fora igangsettes det nå arbeider med risiko knyttet til cybersikkerhet i 5G, herunder kjernenett, drift, vedlikehold og industriapplikasjoner. Risikovurderingene gjennomføres først på nasjonalt nivå. I oktober 2019 skal en koordinert risikovurdering bli gjort på europeisk nivå. Målet er å samle en oversikt over «best practice» for ulike typer risiko og tiltak i medlemslandene. Dette arbeidet kan også eventuelt munne ut i felles europeiske cybersikkerhetskrav til 5G.

4.4 Forskyvning av kompleksitet

I tidligere EkomROS-rapporter har vi beskrevet utviklingstrekk som vi har kalt «fra fysiske til logiske nettverk», «veien mot 5G, virtualisering og automatisering» og «nye muligheter og utfordringer med 5G og IoT». Fellestrekket for alle er kompleksitet, og at denne kompleksiteten flyttes fra ett sted i verdikjeden til et annet. Kompleksitet «forskyves» gjennom å virtualisere, flytte til skyen, ta i bruk skivedeling og overlate beslutninger til kunstig intelligens.

Sett fra én side fører dette til en forenkling, f.eks. ved å erstatte spesialisert maskinvare med hyllevareutstyr, og ekomspesifikke protokoller med standard IT-protokoller. På den annen side blir ikke kompleksiteten mindre. I noen tilfeller er det snakk om nye lag med komponenter eller aktører, mens i andre tilfeller vil deler av produksjonen av ekomtjenester forskyves til et nytt nivå eller et nytt ledd.

Virtualisering av nettfunksjoner

Virtualiseringen innebærer at funksjoner i nettet kan frikobles fra spesialisert utstyr plassert på ett bestemt sted. Dette legger også til rette for at nettverksfunksjoner og tjenesteproduksjon kan flyttes til skyen. Virtualiseringen er i stor grad drevet av to ønsker:

1) *Redusere kostnader generelt, og*
2) *redusere tid for å bringe nye tjenester til markedet.*

Bruk av hyllevare datautstyr i stedet for spesialisert maskinvare, reduserer kostnadene. Sett fra en ekomtilbyders ståsted, kan virtualisering av nettfunksjoner og drift av nettene i skyen, representere en forenkling. Den optimaliseringen som ligger til grunn for effektiv stordrift, skjer imidlertid ikke uten å introdusere ny kompleksitet. Virtualisering krever nye styrings- og kontrollmekanismer som blir levert av ulike leverandører. Slik oppstår lange verdikjeder med flere aktører – som alle skal være med å sikre og ivareta stabilitet og konfidensialtet i tjenestene.

I en første fase vil tilbyderne trolig håndtere virtualisering innenfor sin egen private skyløsning. Det kan være ytterligere effektiviseringsgevinst å hente ved å plassere deler av produksjonen hos en tredjepartsleverandør av skytjenester.

Skivedeling av nett

5G blir markedsført som et nett som kan dekke mange behov. Innen noen områder er lave forsinkelser viktig, innen andre områder vil høy overføringshastighet eller høy pålitelighet være mest avgjørende. I 5G kan en ved hjelp av virtualisering dele et nett i såkalte skiver.

Skivedeling av nett er å opprette flere logiske nett av samme underliggende fysiske nett, ved å bruk virtualiserte nettfunksjoner. Hver skive av nettet kan settes sammen slik at den har egenskaper som er optimalisert for én spesiell anvendelse, for eksempel lav forsinkelse. En annen grunn til å ha en egen skive av nettet, kan være krav til sikkerhet og uavhengighet av andres belastning på nettet. Oppdragskritisk kommunikasjon, som i dagens Nødnett, er en anvendelse det er naturlig å tildele en egen skive.

Skivedeling krever styring ut over det som er beskrevet over, men samtidig henger det nøye sammen. En mobiloperatør må ha god kontroll med sitt nett og inndeling i logiske skiver for ulike kunder eller anvendelsesområder. Men på ett eller annet nivå i virtualiseringshierarkiet, er det sannsynlig at andre aktører vil kunne komme inn og tilby mer spesialisert kompetanse.

Software-defined networking

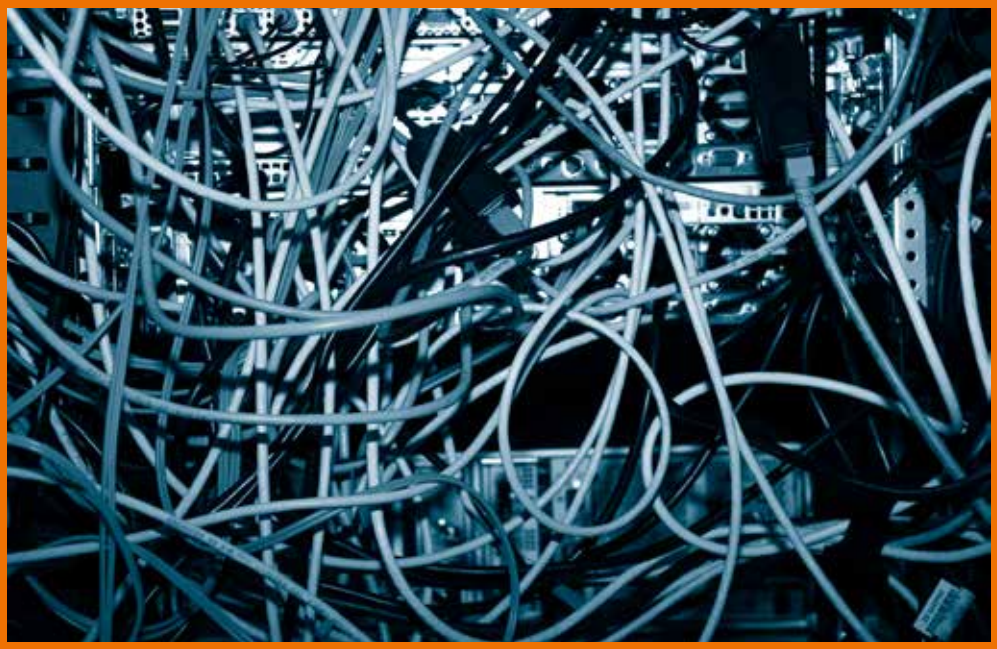
Software-defined networking (SDN) er en komplementær teknologi til virtualisering av nettfunksjoner. Begge teknologier understøtter bransjens behov for raske omstillinger i nettene. SDN handler om å skille kontroll av trafikk fra selve flyten av nyttetrafikk. Å skille mellom disse to typene kommunikasjon er ikke nytt i elektronisk kommunikasjon, men SDN gjør det mulig å sentralisere konfigurering og kontroll av nettene og gjøre konfigurering mer dynamisk enn før. En trenger altså å kunne håndtere kompleksiteten knyttet til dynamisk rekonfigurering, i tillegg til det som har med trafikkstyring å gjøre.

Tjenestebasert arkitektur

Mobilnettene opp til og med fjerde generasjon (4G) er bygd opp slik at de ulike nettelementene kommuniserer over ekom-spesifikke protokoller og grensesnitt. Her er meldinger bygd opp med dataformater som er mest brukt i telekommunikasjon. I 5G står vi overfor en såkalt tjenestebasert arkitektur, hvor tjenester kan nås via standard programmeringsgrensesnitt og hvor meldinger har et format som er utbredt for IT-systemer. Kompleksiteten flytter seg fra én type arkitektur, som er kjent og forstått av relativt få (4G), til én arkitektur som har langt større utbredelse (5G). Dette innebærer at flere potensielt kan utnytte svakheter, men også at flere ressurser er tilgjengelig for å utvikle beskyttelsesmekanismer.

Kunstig intelligens

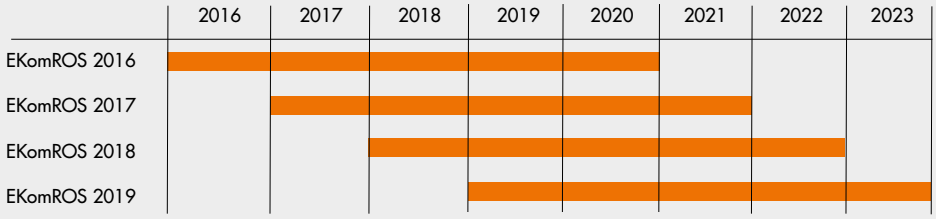
Kunstig intelligens er programvare som er inspirert av måten mennesker lærer og handler på. Programvaren er designet for å lære av omgivelsene og tilpasse handlinger etter forholdene istedenfor å være statisk programmert til å utføre en bestemt oppgave. Innenfor elektronisk kommunikasjon kan kunstig intelligens automatisere stadig flere oppgaver innen kundebehandling, provisjonering, nettverkskonfigurasjon, feildiagnostisering, osv. Produksjonen av ekomtjenester vil bli avhengig av kompetanse som ligger på siden av den som tilbyderne tradisjonelt har hatt, og enkelte feilsituasjoner vil måtte løses ved hjelp av kompetanse på kunstig intelligens.



5

RISIKOVURDERING

De årlige EkomROSene kompletterer hverandre slik at de over noen år til sammen fanger opp de vesentligste og overordnede sikkerhetsutfordringene i sektoren.



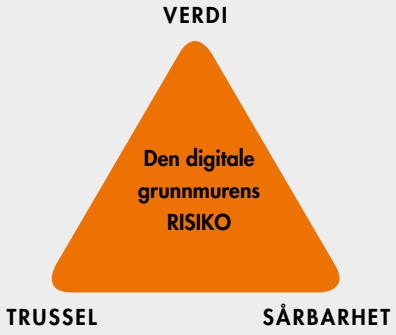
Figur 5 - De årlige vurderingene av fremtidig risiko kompletterer hverandre

Ekomloven stiller krav til at ekomnett og -tjenester skal ha innebygget forsvarlig sikkerhet for brukerne i fred, krise og krig.
I den overordnede risikovurderingen tar derfor Nkom hensyn til uønskede hendelser i hele krisespekteret, både utilsiktede og tilsiktede, og samtidig tilgjengelighet, integritet og konfidensialitet for ekomnett og -tjenester.

EkomROS legger først og fremst vekt på å skape oppmerksomhet om aktuelle risikoområder innenfor ekomsektoren. Det er den enkelte aktørs selvstendige ansvar å gjennomføre konkrete risikovurderinger for egen virksomhet og iverksette risikoreduserende tiltak som gir forsvarlig sikkerhet i nett og tjenester.

Risiko kan beskrives på ulike måter, avhengig av hvilken kontekst risiko skal vurderes ut fra. I årets EkomROS tar Nkom utgangspunkt i den såkalte «risikotrekanten»:

- *Hvilke verdier kommer den digitale grunnmuren til å bære de kommende år?*
- *Hvilke trusler og farer står ekomsektoren overfor?*
- *Hvilke sårbarheter vil dukke opp som følge av overgangen fra gammel til ny teknologi?*



Figur 6 - Risikotrekanten

5.1 Den digitale grunnmuren skal bære store SAMFUNNSVERDIER

Den teknologiutviklingen vi står midt oppe i vil berede grunnen for en eksplosiv digitalisering innenfor alle kritiske samfunnsfunksjoner de nærmeste årene; fra landets styringsevne og suverenitet, til helse og omsorg, nød- og beredskapstjenester, finansielle tjenester og til forsyning av kraft, vann og avløp.

Dette vil styrke koblingen mellom den digitale grunnmuren og de samfunnsverdiene som legges på grunnmuren. DSB deler samfunnsverdiene opp i liv og helse, natur og miljø, økonomi, samfunnsstabilitet og demokratiske verdier og styringsevne. Eksemplene på denne koblingen er mange:

- **Liv og helse:**
  I 2017 besluttet regjeringen at fremtidens nød- og beredskapstjenester skal realiseres i de kommersielle mobilnettene, og ikke i et dedikert mobilnett tilsvarende dagens Nødnett. Dette vil gi nød- og beredskapsbrukerne mulighet til å dra nytte av den høye innovasjonstakten og tjenesteutviklingen i de kommersielle nettene. Beslutningen illustrerer også forventningen om, og tilliten ti,l at de kommersielle nettene vil opprettholde et forsvarlig sikkerhetsnivå.

- **Økonomi:**
  Finanstilsynets risiko- og sårbarhetsanalyse peker på digitaliseringsbølgen innenfor finanssektoren: «Den teknologiske innovasjonen endrer næringen gjennom nye løsninger, økt konkurranse og nye aktører i verdikjedene. Progresjonen i utviklingen innen kunstig intelligens, maskinlæring, robotisering, økt bruk av stordata samt ny teknologi som blokkjede og bruk av skytjenester, bidrar til en digitaliseringsbølge som påvirker og utfordrer foretakenes forretningsmodeller.»[18]

- **Demokratiske verdier og styringsevne:**
  Den gjeldende langtidsplan for forsvarssektoren legger opp til i økende å grad benytte sivile leverandører til IKT-infrastruktur og tjenester. Forsvarssjefens fagmilitære råd til langtidsplanen er at «[de] oppgavene kun Forsvaret kan løse og som definerer Forsvarets kjernevirksomhet, vil bli prioritert. Informasjonsinfrastrukturen utvikles kontinuerlig videre, og nye løsninger må i større grad fremskaffes, basert på tilpasning og forbedring av eksisterende infrastruktur. I tillegg må løsningene suppleres med tilgjengelig militær og sivil teknologi.»[19] *For eksempel har Forsvarsmateriell (FMA) allerede pilotprosjekter i gang for å utvikle løsninger for sikker mobilkommunikasjon i Forsvaret gjennom kommersielle mobilnett.*

Digitaliseringen i de ulike samfunnssektorene forutsetter ekomnett og -tjenester som alltid er tilgjengelige, som ivaretar integriteten i kommunikasjonen, og som ivaretar konfidensialiteten til informasjonsverdiene som blir formidlet, prosessert og lagret. I nasjonal strategi for digital sikkerhet, skriver statsminister Erna Solberg:

«Det forventes at digitale tjenester skal være tilgjengelige til enhver tid. En vellykket digitalisering handler også om at løsningene ivaretar krav til sikkerhet og den enkeltes personvern på en god måte, og at vi kan ha tillit til at digitale løsninger fungerer slik de skal.»[20]

[18] *«Risiko- og sårbarhetsanalyse (ROS) 2017», Finanstilsynet, mai 2018*
[19] *«Et forsvar i endring – forsvarssjefens fagmilitære råd», Forsvaret, 2015*
[20] *«Nasjonal strategi for digital sikkerhet», Departementene, 2019*

5.2 En vedvarende TRUSSEL

Trusselaktørenes muligheter for å ramme virksomheter, infrastrukturer og tjenester innen elektronisk kommunikasjon er mange. Som et eksempel har Forsvarets forskningsinstitutt benyttet en metodikk[21] for å analyse mulighetene for tilsiktede uønskede handlinger rettet mot Forsvarets informasjonsinfrastruktur. Her identifiserer de 900 ulike kombinasjoner av overordnede angrepsmetoder som kan ramme informasjonsinfrastrukturens verdier som informasjon, tekniske systemer eller menneskelige prosesser. Hver angrepsvektor kan deles inn i mange underkategorier, kombineres på ulike måter, og gjennomføres i ulike kontekster (freds-, krise-, eller krigsscenarioer), noe som i realiteten skaper nærmest uendelige kombinasjoner.

Tilsiktede uønskede handlinger

Det overordnede trusselbildet beskrevet i kapittel 4, viser et bredt spekter av trusler, både i det digitale rom (etterretning, kartlegging, nettverksoperasjoner og påvirkningsoperasjoner), innenfor menneskelige prosesser (innsidere) og strategiske prosesser (oppkjøp og investeringer) og rene «maktdemonstrasjoner» som jamming.

I noen tilfeller er det ekomnett og -tjenester som bærer truslene. Det vil si at de er rettet mot brukerne, som virksomheter og industri, gjennom nettverksoperasjoner som skadevare, tjenestenektangrep osv. Denne typer trusler er sektorovergripende og gjelder ikke særskilt for ekomsektoren.

I andre tilfeller er truslene rettet mot tilbyderne av ekomnett og -tjenester, slike som mobil- og bredbåndsselskap. I lys av de stadig økende samfunnsverdiene som forvaltes i de elektroniske kommunikasjonsnettene, anser Nkom at trusselaktørenes vilje til å rette oppmerksomheten mot selve den digitale grunnmuren vil øke. Særlig oppmerksom mener Nkom man bør være på fordekte digitale eller menneskelige operasjoner som har til hensikt å påvirke nett og -tjenesters integritet og konfidensialitet.

Trusseltype og omfang som ventes å være rettet mot ekomnett og -tjenester vil være avhengig av trusselaktøren. Når man ser hvilken betydning cyberdomenet har fått for den internasjonale sikkerhetspolitikken, må man forutsette at det finnes trusselaktører med både vilje, evne og kapasitet til å gjennomføre svært avanserte operasjoner for å etablere seg «på innsiden».

I tillegg må vi forvente at avdekte sårbarheter i økende grad vil utnyttes til økonomisk vinning, for eksempel kryptolåsing.

Man skal heller ikke undervurdere avanserte trusselaktørers evne og vilje til å påvirke nett og tjenesters tilgjengelighet gjennom å demonstrere evnen til å slå ut kritiske tjenester, slik man har sett i enkelte tilfeller av GNSS-forstyrrelser i Nord-Norge. Denne type hendelser kan både skape frykt og redusere samfunnets og brukernes tillit til bestemte nett, tjenester eller systemer.

Naturhendelser og ulykker

Uønskede hendelser inkluderer også utilsiktede hendelser. Det er også disse hendelsene som påvirker den digitale grunnmuren mest i det daglige, gjennom påkjenninger som følger av naturhendelser og gjennom tekniske og menneskelige feil.

Nkom legger til grunn at man fremover må forvente mer ekstremvær og flom, som kan utløse strømbrudd, fiberbrudd og fysisk skade på anlegg. For øvrig må man være oppmerksom på andre store hendelser og ulykker, som direkte eller indirekte kan påvirke tilgjengelighet og stabilitet til ekomnett og -tjenester. DSBs analyser av krisecenarioer[22]

---

[21] *«En morfologisk analyse av tilsiktede uønskede handlinger rettet mot Forsvarets informasjonsinfrastruktur», Forsvarets forskningsinstitutt, 2018.*

[22] *«Analyser av krisecenarioer 2019», DSB, 2019*

tar blant annet for seg ekstremvær og flom, pandemi, romvær (solstorm), strømrasjonering og terrorangrep. Når samfunnet om få år er enda mer gjennomgående digitalisert, vil håndteringen av slike hendelser i enda større grad forutsette fungerende ekomnett og -tjenester. Dersom hendelsene samtidig påvirker den digitale grunnmurens funksjon, vil konsekvensbildet fort bli verre.

5.3 Digitaliseringsveksten skaper nye SÅRBARHETER

Sårbarhetene som oppstår i overgangsperioden når ny teknologi og nye sikkerhetsløsninger skal implementeres, og samtidig skal samvirke med eldre teknologi, må ikke undervurderes.

Økt kompleksitet – nye aktører - flere angrepsflater

Teknologiutviklingen innenfor elektronisk kommunikasjon innebærer på mange områder store forbedringer på sikkerhetsfeltet. Samtidig vil kompleksiteten i programvare i de elektroniske kommunikasjonsnettene øke betraktelig. Nye tjenester med krav til svært lave forsinkelser vil kunne medføre at enkelte applikasjoner logisk vil plasseres ute i tilgangsnettet nærmere brukerne. Med disse endringene kommer også nye tredjeparts aktører inn i verdikjedene. Samlet innebærer dette en betydelig økning av både logiske og fysiske angrepsflater, og et økt potensiale for utilsiktede sikkerhetsbrister og uventede feil. Dette kan ramme systemenes integritet, konfidensialitet og tilgjengelighet.

Å sikre seg slik at en kan forhindre alle mulige angrepsvektorer som kan ramme den digitale grunnmuren, bestående av elektroniske kommunikasjonsnett og -tjenester med dens komplekse avhengigheter og verdikjeder, er en umulig oppgave.

Olav Lysne beskriver i sin bok «The Huawei and Snowden Question» hvordan det på de fleste nivåer i programvareutvikling er en umulig oppgave å sikre fullstendig integritet. Det er ikke mulig å bevise at et element eller en funksjon i nettet, av en viss kompleksitet, ikke gjør noe i tillegg til det den skal gjøre, for eksempel å avlytte en samtale, ødelegge seg selv på et tidspunkt eller ha en bakdør for tilgang til vitale systemfunksjoner. Det vil, ifølge Lysne, være mulig for en produsent å legge inn slike uønskede egenskaper uten at vi i praksis kan oppdage det.

Særlig bekymringsfulle er derfor de sårbarhetene som skjules av de elektroniske kommunikasjonsnettenes kompleksitet. Avanserte trusselaktører kan i det skjulte utnytte dette for etterretning, informasjonsuthenting og manipulering.

Manglende oversikt over hvordan de ulike leddene i verdikjeden påvirker hverandre, kan også gi seg utslag i utilsiktede sikkerhets- og tilgjengelighetsbrudd. Hvordan en tilsynelatende triviell feil i en verdikjede kan få store konsekvenser, så vi et eksempel på i desember 2018. Et titalls millioner mobilabonnenter hos mobiloperatører i Storbritannia, Japan og i ni andre land, mistet mobiltjenestene. Årsaken var et utgått sikkerhetssertifikat i en programvare på en kjernenode som var i disse operatørenes nett.[23] Hendelsen eksemplifiserer også sårbarheter knyttet til å være avhengig av enkeltleverandører og understreker behovet for leverandørdiversitet i kritiske systemer.

«Ettermontert» sikkerhet på gamle løsninger

Selv om nye systemer og løsninger bygger sikkerhet inn allerede i designfasen, er man fortsatt svært avhengig av eldre og helt grunnleggende protokoller som skal sikre at telekommunikasjon og internett fungerer på tvers av nettverk og landegrenser. Mange av disse protokollene ble utviklet i en tid da tillit-

[23] *https://www.ericsson.com/en/press-releases/2018/12/update-on-software-issue-impacting-certain-customers?hootPostID=ef3d37949fba5349b993945f911d89e6*

en mellom de kommuniserende partene var stor. I dag kan ikke lenger denne tilliten uten videre legges til grunn.

Tilbyderne jobber derfor med å bygge inn mekanismer for å kunne kontrollere og verifisere både integritet og autentisitet i disse systemene og protokollene. Ved å utvide de gamle protokollene med ny sikkerhetsfunksjonalitet, «ettermonteres» sikkerheten. Dette sikrer at nye metoder fortsatt er kompatible med de eldre systemene. Eksempler på slike sikkerhetsmekanismer er:

- *DNSSEC; sikkerhetsmekanismer bygd inn i domenenavnsystemet (DNS) for å hindre muligheten for å injisere falske svar i domenenavnoppslag, som kan utnyttes for eksempel til å stjele informasjon eller manipulere transaksjoner.*
- *RPKI og BGPSEC; sikkerhetsmekanismer bygd inn i rutingprotokollen som benyttes i kjernen av Internett (BPG) som benytter elektronisk signering av ressurser for å motvirke feilkonfigurasjon, og for å motvirke bevisst manipulering av rutingen av internettrafikken.*
- *Tiltak for å sikre SS7: Sikkerhetsmekanismer som er bygd på signaleringsprotokollen SS7 som styrer sammenkobling av samtaler mellom telekommunikasjonsnett, for å hindre muligheten for sporing, manipulering og avlytting.*

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

Menneskelige faktorer og kompetansebehov ved endring

Vi står på mange måter foran et paradigmeskifte i sektoren i lys av de kommende teknologiendringene. Løsninger som før har benyttet ekomspesifikke teknologier og protokoller, går nå i retning av standardiserte løsninger vi kjenner fra IT- og internettdomenet. Dette innebærer også et betydelig behov for ny og oppdatert kompetanse hos nettoperatørene. Mer enn å erstatte et ekom-miljø med et IT-miljø, er det heller snakk om å få til en sammensmelting av miljøene.

Med de omfattende teknologiendringene som vi nå står overfor, forventer Nkom derfor at nye feilsituasjoner og sikkerhetsbrister vil forekomme i en overgangsperiode, inntil løsningene modnes, og nyervervet kompetanse hos ekomtilbyderne forsterkes av erfaring.

Skepsis til ny teknologi

Tillit er avgjørende for digitaliseringen - tillit til at systemene fungerer, at de er tilgjengelige, og at de ivaretar integritet og konfidensialitet for brukerne. Men digitaliseringen forutsetter også tillit til at teknologien i seg selv ikke er helseskadelig. Ved de fleste teknologiskifter som innebærer trådløs kommunikasjon, oppstår spørsmål om den elektromagnetiske strålingens effekt på mennesker. Bekymringen er ytret under alle teknologiskifter på mobil; fra 2G, 3G, 4G og nå ved innføringen av 5G. Det samme gjelder for utrullingen av Nødnett, smarte strømmålere (AMS) og DAB.

Det foregår mye forskning og undersøkelser på feltet. Nkom har også gjennom mange år målt og dokumentert nivåene av den samlede dekning/stråling der folk normalt ferdes og oppholder seg over tid, og delt resultatene med offentligheten. Nkom anser det som svært viktig å holde fram med å utvikle gode målemetoder og kartlegge strålenivåer også for 5G, for å gi god faglig og objektiv informasjon både til andre myndigheter og direkte til befolkningen.

5G og reservestrøm

Strømforsyning og elektronisk kommunikasjon er gjensidig avhengig av hverandre. Sårbarhetene som ble avdekket etter ekstremværet Dagmar i 2011, utløste flere tiltak. To av de sentrale var minstekrav til reservestrøm i mobilnett og oppgraderingsprogrammet Forsterket ekom. I dette får flere kommuner hvert år etablert ett kommunikasjonspunkt med minst tre døgn reservestrøm og forsterket transmisjon til basestasjoner. Programmet er finansiert i samarbeid mellom staten og mobilnetteierne, og gir dekning i strategisk viktige områder i kommunene. Slik blir evnen til krisehåndtering betydelig hevet.

Minstekravene til driftstid i mobilnettene ved strømutfall er ikke knyttet til spesifikke mobilteknologier. Mobiloperatørene må derfor ta hensyn til kravene også når de skal bygge ut 5G.

For å innfri de høye båndbreddene i 5G, må samfunnet ta i bruk flere frekvenser i høyere frekvensbånd. Det vil bli etablert langt flere «kapasitetsantenner» nærmere brukerne, for eksempel på husvegger og i lyktestolper. I motsetning til de større «dekningsbasestasjonene», vil nok mange av disse ikke ha store batteripakker for reservestrøm, noe som kan føre til betydelig kapasitetstap ved strømbrudd.

Minstekravene til driftstid gjelder ikke overalt. For eksempel gjelder ikke dagens krav for innendørsdekning, et dekningsområde som er svært viktig for 5G. Det er viktig at både myndighetene, mobiloperatørene og virksomheter som ønsker å benytte nettet til potensielt kritiske formål, er bevisst sårbarheten og ansvarsfordelingen ved brudd i strømforsyningen når stadig flere prosesser i samfunnet digitaliseres.

Bruk av satellitt som synkroniseringskilde i 5G

De siste par årene har samfunnets sårbarhet overfor jamming og narring/spoofing av GNSS[24] vært på dagsorden. Nkom vil rette oppmerksomheten mot denne tematikken, fordi det er høye krav til synkronisering av tid og takt i nettene for å oppnå høy datakapasitet. Synkronisering i 5G kan i prinsippet bli løst enten gjennom kun å hente nøyaktig tid og takt via GNSS på basestasjonene, eller gjennom fibernettet, eller ved å bruke de to metodene sammen som primær- og sekundærkilder. Metodevalg avhenger av hvilke løsninger utstyrsleverandørene tilbyr, hvilke fiber-/klokkeinfrastruktur mobiloperatørene selv har, kost-/nyttevurderinger og eventuelle myndighetskrav.

Det er på det rene at dersom 5G-nettene utelukkende baserer seg på tid og takt fra GNSS, så introduserer det en betydelig sårbarhet. Dette gjelder både tilsiktede hendelser som jamming og spoofing, og utilsiktede hendelser som solstorm og teknisk svikt.

Nkom er i dialog med både de norske mobiloperatørene og de nordiske teletilsynene om denne problematikken. Dette er også i tråd med en ny nasjonal strategi, hvor det fremkommer at regjeringen vil *«vurdere evnen til å opprettholde nøyaktig tid i digitale nett og om det er hensiktsmessig å innføre nasjonale krav til hvor lenge slike nett bør kunne fungere ved svikt i GNSS.»*[25]

5.4 Samlet risikovurdering

I årets EkomROS har vi skildret en digital grunnmur som per i dag, og i enda større grad i fremtiden, utgjør en kritisk samfunnsfunksjon og som skal bære og forvalte store mengder informasjon og samfunnsverdier.

Den digitale grunnmuren er et høyverdig og vedvarende mål for trusselaktører, enten det gjelder etterretning, nettverksoperasjoner eller vinningskriminalitet. Den digitale infrastrukturen vil også bli påvirket av naturhendelser, strømbrudd og uforutsette tekniske og menneskelige feil.

Den betydelige kompleksitetsveksten vi står overfor, særskilt oppmerksomhet. Den gjør det utfordrende å kartlegge og forutse potensielle sårbarheter, uønskede hendelser og deres konsekvenser.

---

24 Global Navigation Satellitte Systems
25 «På rett sted til rett tid - nasjonal strategi for posisjonsbestemmelse navigasjon og tidsbestemmelse», Samferdselsdepartementet, 2018


NKOM
Nasjonal kommunikasjonsmyndighet

6

RISIKOHÅNDTERING

Den digitale grunnmuren må ha evne til å opprettholde, og eventuelt raskt gjenopprette sine funksjoner, også når den utsettes for ukjente og uforutsette påkjenninger. Den digitale grunnmuren må være resilient.[26] Resiliens beskriver et systems motstandsdyktighet og tilpasningsevne til å opprettholde eller raskt gjenopprette funksjon, selv om systemet blir satt under press.

Nkom anser følgende tiltakskategorier som viktige for å bygge en resilient digital grunnmur:

- **Økt diversitet:**
  Systemer som baserer seg på flere og uavhengige fysiske lokasjoner og traséer, uavhengige teknologier og leverandører, og uavhengige operasjonelle systemer og løsninger.
- **Responsevne:**
  Evne til å avdekke og håndtere digitale hendelser gjennom å videreutvikle samarbeid mellom responsmiljøer.
- **Beredskap:**
  Evne til å være forberedt for uforutsette hendelser forårsaket av for eksempel klimaendringer eller ondsinnede aktører.
- **Kompetanse:**
  Tilstrekkelig teknologi- og sikkerhetskompetanse til å forstå den økte kompleksiteten i verdikjedene som inngår i produksjon av ekomtjenester.

Flere av disse momentene inngår i regjeringens nye nasjonale strategi for digital sikkerhet. Nkom mener de norske elektroniske kommunikasjonsnettene, som utgjør den digitale grunnmuren, har et godt utgangspunkt for å møte risikobildet vi står overfor. Det vil imidlertid kreve vedvarende innsats på sikkerhetsområdet.

Regjeringens strategi setter også søkelys på sikkerhetsarbeidet hos myndighetene og brukerne av den digitale grunnmuren. Bevissthet rundt ansvaret for egen sikkerhet vil også være avgjørende for at digitaliseringen skal lykkes.

[26] *"Resiliens – hva er det og hvordan kan det integreres i risikostyring?", Forsvarets forskningsinstitutt (FFI), 2019*

07 MEDIA 392078 Foto: Nkom

Besøksadresse:
Nygård 1, Lillesand

Postadresse:
Postboks 93,
4791 Lillesand

Tlf: 22 82 46 00

nkom.no