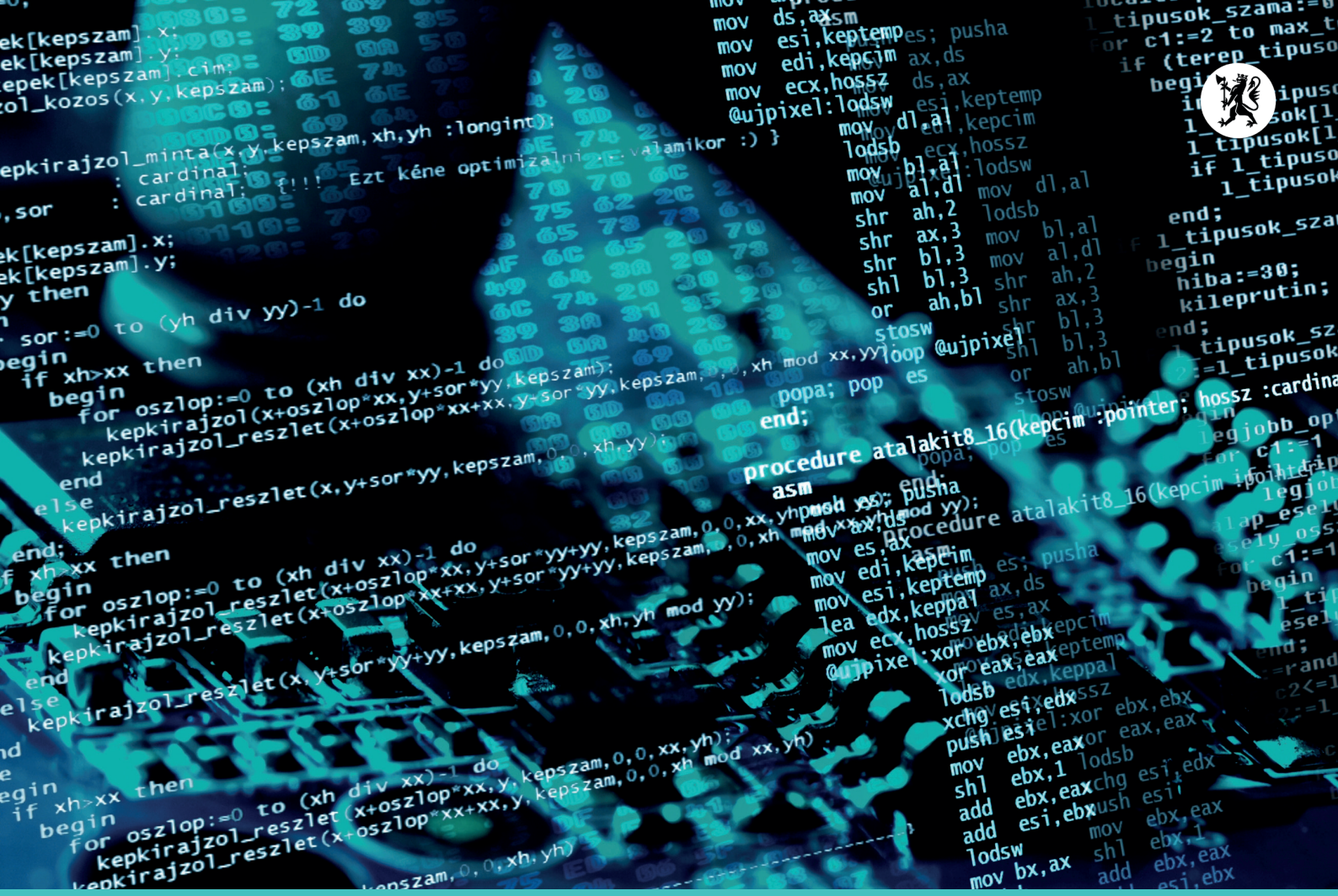


6. Digitale sårbarheter

> Scenario: Utpressingsangrep mot kommuner og interkommunalt IKT-samarbeid

> Elektronisk kommunikasjon (EKOM)

Innledning

Norge er et av de mest digitaliserte landene i verden. Utviklingen skaper imidlertid sårbarheter. Stadig flere enheter, prosesser og tjenester kobles sammen og til internett. Dette medfører digitale verdikjeder som er lange, komplekse, uoversiktlige og ofte internasjonale til dels utenfor norske myndigheters kontroll. Den digitale flaten som kan utsettes for angrep vokser.[63]

Digitale angrep skjer kontinuerlig og utgjør en stor utfordring for samfunnet og mange virksomheter. De fleste digitale angrep vil være nettverksbaserte, det vil si at de utnytter de mulighetene som ligger i at datasystemer er koplet sammen i et globalt nettverk. Handlingene er ofte politisk eller økonomisk motivert. For systemer som er adskilt fra omverdenen og ikke kan nåes gjennom nettverksbaserte operasjoner, vil bruk av innsidere være den mest effektive angrepsmetoden.[64] [65]

Sommeren 2023 ble det kjent at 12 norske departementer var blitt kompromittert gjennom bruk av nulldagssårbarheter. Nulldagssårbarheter er i praksis nesten umulige å beskytte seg mot. De kjøpes og selges på digitale undergrunnsmarkeder, hvor en symbiose av hackere, kriminelle og etterretningstjenester opererer. Men det hjelper alltid, uansett, å installere sikkerhetsoppdateringer så raskt som mulig, og ha orden på loggfiler.[66]

Temaboks: Innsiderisiko

Innsiderisiko handler om personer som kan komme til å utnytte sine legitime tilganger til virksomhetens verdier for uautoriserte formål. En innsider kan være en nåværende eller tidligere ansatt, konsulent eller innleid, som har eller har hatt en legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne tilgangen på en måte som påfører virksomheten tap eller skade.

En ubevisst innsider er en innsider uten intensjon. Handlinger som begås av ubevisste innsidere henger ofte sammen med lav sikkerhetsmessig bevissthet hos den aktuelle personen, samt mangelfull sikkerhetsstyring og daglig sikkerhetsmessig ledelse i virksomheten.

Se NSM temarapport innsiderisiko

[63] DSB, Analyser av krisescenarioer 2019, s. 197
[64] DSB, Analyser av krisescenarioer 2019, s. 197
[65] Kripos, Politiets trusselvurdering 2023, s. 29
[66] NSM, Nasjonalt digitalt risikobilde 2023, s.10

Scenario: Utpressingsangrep mot kommuner og interkommunalt IKT-samarbeid

Klokken 07:50, torsdag 25. desember meldes det inn fra hjemmesykepleien til IKT-samarbeidet at de har mistet påloggingstilgang til sine fagsystemer. Tilgangen har manglet i noen timer allerede, men det er usikkerhet nøyaktig på hvilket tidspunkt i løpet av natten tilgangene forsvant. IKT-samarbeidet starter arbeid med feilsøking og kartlegging av feil og omfang. Innledende undersøkelser viser at systemene er nede, og at det har vært uvedkommende inne i systemene.

Undersøkelsene viser videre at omfanget av hendelsen sprer seg utover fagsystemene til hjemmesykepleien i kommune #1. Videre kommer det nå også inn lignende varsler fra to andre kunder, henholdsvis kommune #2 og Agder fylkeskommune, om at også de har mistet tilgang til sine datasystemer.

IKT-samarbeidet arbeider med å kartlegge omfanget av berørte systemer og forsøker å gjenopprette tilganger, uten hell. Klokken 11 kommer det en melding fra en ukjent aktør til daglig leder i IKT-samarbeidet og kommuneledelsen om at en hackergruppe ved navn «hackLOvE» har gjennomført et nettverksangrep, og gjennom flere måneder har arbeidet for å tilegne seg administratortilganger og informasjon.

Gruppen har tilegnet seg sensitive person-, og saksopplysninger, inkludert kontakt- og adresseinformasjon til kommunens ansatte, og sårbare brukergrupper (herunder pasientjournaler).

Gruppen krever at kommunene betaler en million kroner (for hver kommune) i en spesifisert kryptovaluta til en crypto-wallet (ukjent bankkonto). Frist for gjennomføring av krav settes til klokken 18.00 samme kveld. Dersom kravene ikke innfris vil gruppen legge informasjonen ut for salg på det mørke nettet, og dersom kommunene deretter ikke innfrir kravene innen midnatt vil informasjonen publiseres åpent på sosiale media og internett. Videre vil gruppen slette utvalgte sikkerhetskopier, informasjon og tilganger.

Gruppen informerer videre om at dersom kommunene velger å betale den «rimelige økonomiske summen» vil gruppen gjenopprette alle tilganger, og eventuelt ødelagte data.

Det er ikke mulig å besvare meldingen som ble sendt til IKT-samarbeidet og kommuneledelsene.

Sårbarhet

Flyktigheten i det digitale markedet der leverandører byttes ut, selskaper kjøpes opp, ny teknologi oppstår og gammel raskt byttes ut, bidrar til å komplisere bildet ytterligere. En slik sårbarhet er uoversiktlig og uforutsigbar.[67] De sårbarhetene Nasjonal sikkerhetsmyndighet (NSM) oftest finner hos norske virksomheter er dårlige passord, slurv med tilganger og utdaterte systemer.[68]

Samfunnsstabilitet

Dataangrep mot kritiske samfunnsfunksjoner kan få konsekvenser i store deler av samfunnet. Dette gjelder særlig dersom kraftforsyningen eller elektronisk kommunikasjon rammes. Ukraina har blitt utsatt for slike cyberangrep gjentatte ganger: I 2015, 2016 og sist i februar 2023. I februar førte angrepet mot energisystemer til strømutfall i store områder. Løsepengeangrepet mot Colonial Pipeline i USA i 2021 medførte betydelige samfunnskonsekvenser, da distribusjon av drivstoff stanset opp. SolarWinds-angrepet i 2020 fikk nasjonale konsekvenser da norske kraftselskaper ble berørt. Alle disse hendelsene viser kompleksiteten i systemer og nettverk i kritisk infrastruktur, og hvor store samfunnskonsekvenser et cyberangrep kan medføre.

Usikkerhet

Krig i Europa skaper usikkerhet, og gjør fremtiden vanskelig å forutse. Usikkerheten forsterkes ytterligere av en teknologisk utvikling med stadig hurtigere tempo og utbredelse. Kunstig intelligens utfordrer vår evne til å se forskjell på ekte og falskt, på sant og usant. Vi har allerede sett at mulighetsrommet for maskingenerert kreativitet er stort. Hvor stort det vil være om ett år eller mer, er vanskelig å si. Potensialet for å bruke teknologien i det godes tjeneste er stort. NSM ser med bekymring på potensialet for det motsatte. Alt som kan brukes, vil misbrukes.

---

[67] DSB, Analyser av krisescenarioer 2019, s. 197

[68] NSMs Grunnprinsipper for IKT-sikkerhet, versjon 2.0. s.16-17

Risikovurdering

På nasjonalt nivå mener NSM at informasjonssystemer som understøtter grunnleggende nasjonale funksjoner ikke er tilstrekkelig kartlagt, og ofte ikke har etablert et forsvarlig sikkerhetsnivå.

Mulige risikoreduserende tiltak[69]

For å ivareta god egensikkerhet er det et godt utgangspunkt å basere arbeidet på anbefalingene fra blant annet NSMs Grunnprinsipper for IKT-sikkerhet, verdiene som organisasjonen forvalter, egne risiko- og sårbarhetsvurderinger, samt eksponering (tiltrekningskraft) fra omgivelsene.

- Installere sikkerhetsoppdateringer så raskt som mulig, og ha orden på loggfiler for å sikre sporbarhet og historikk. Manglende sikkerhetsoppdateringer skaper unødvendige sårbarheter og en logg har liten verdi om den aldri sjekkes.
- Ta i bruk rammeverk som ISO 27001 og/eller NSMs grunnprinsipper som en del av virksomhetens internkontroll.
- Multifaktorautentisering (MFA). Denne sikkerhetsmekanismen har i mange år vært – og er fortsatt – blant de viktigste tiltakene NSM anbefaler.
- Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter. Jevnlig revisjon av brukere og tilganger.
- Etabler retningslinjer for tilgangskontroll.
- Minimer rettigheter til sluttbrukere og spesialbrukere.
- Etabler sikkerhetsovervåkning.
- Kartlegg brukere og behov for tilgang.

[69] Se NSMs Grunnprinsipper for IKT-sikkerhet, versjon 2.0.

Elektronisk kommunikasjon (ekom)

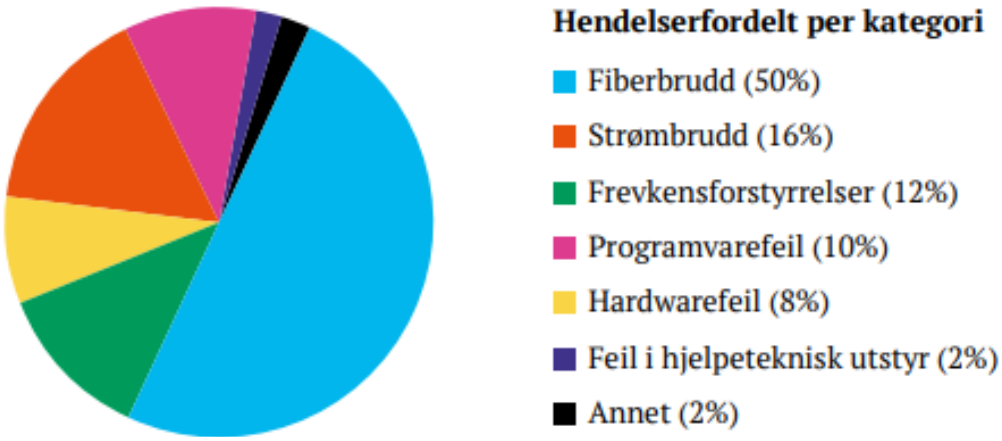
Samfunnets avhengighet av elektronisk kommunikasjon (ekom), og sårbarheten som kan oppstå, er sterkt økende. Digital teknologi har gjort kommunikasjon enklere og billigere, effektivisert produksjon og skapt en rekke nye produkter og tjenester. Anvendelse av digital teknologi griper inn i de fleste områdene i privat og offentlig sektor. Samfunnet forventer også å løse utfordringer i helsesektoren med digital velferdsteknologi. Alt skjer med en slik hastighet at kravene til robusthet ofte kommer i kjølvannet av innføringen av ny teknologi. I løpet av de ti siste årene har gjennomsnittshastighet for internettilknytninger blitt ti ganger høyere. Fra 2003 – 2017 var ekomsektoren sitt bidrag til den gjennomsnittlige årlige produktivitetsveksten i norsk økonomi ca. 40 %. For å opprettholde og utvikle digitale tjenester og produkter, trenger vi faste og mobile nett med tilstrekkelig kapasitet, robusthet og uavhengighet.

En del sårbarhet oppstår når man ikke har tilstrekkelig oversikt, helhetsforståelse og kan se sammenhenger. For å motvirke denne utviklingen mener mange at man må bli flinkere til å dele informasjon om infrastruktur, sårbarheter, evalueringer, KIKS og gjennom kunnskap og helhetsforståelse finne de beste løsningene på en helhetlig og bærekraftig måte. Ekomportalen, hvor kommunene skal registrere all infrastruktur i kommunen, åpner for bedre planlegging og samhandling om robuste løsninger. I Agder er det gjort mange tiltak for å møte disse utfordringene på en systematisk og helhetlig måte.

Hendelser og årsaker

Alvorlige naturhendelser, ekstreme værforhold, bortfall av kraft og villede handlinger utgjør de største truslene mot ekominfrastrukturen.[70]

[70] Nkom – EkomROS 2021



Figur 14: Nkom, 2021: Prosentvis antall ekomutfall rapportert til Nkom fordelt på hendelseskategorier.

NSM viser til at hendelser som medfører utfall av ekomtjenester i Norge kan forekomme som følge av digitale angrep, selv om det er stort fokus på sikkerhet i sektoren.[71]

Roller og ansvar

I Norge er det Kommunal- og distriktsdepartementet (KDD) som har sektoransvaret for ekom.[72] Nasjonal Kommunikasjonsmyndighet (Nkom) er tilsyns- og forvaltningsmyndighet for tjenestene innenfor post og ekom i Norge.[73] [74]

Tilbydere er ansvarlige for å sørge for at nett og tjenester holder et forsvarlig sikkerhetsnivå. I Agder er det Telenor, Telia og ICE som er de største tilbyderne. Tjenestene og nettet skal være tilgjengelige, i tillegg til at integritet og konfidensialitet skal beskyttes. Tilbydere må også ha, og opprettholde nødvendig beredskap. Det gjelder i fred, kriser og krig.[75] [76] [77]

Kobbernettet til Telenor, som har vært hovednett for fasttelefoni og bredbånd skal fases ut. Telenor har leveringsplikt på offentlig telefontjeneste og digitalt elektronisk

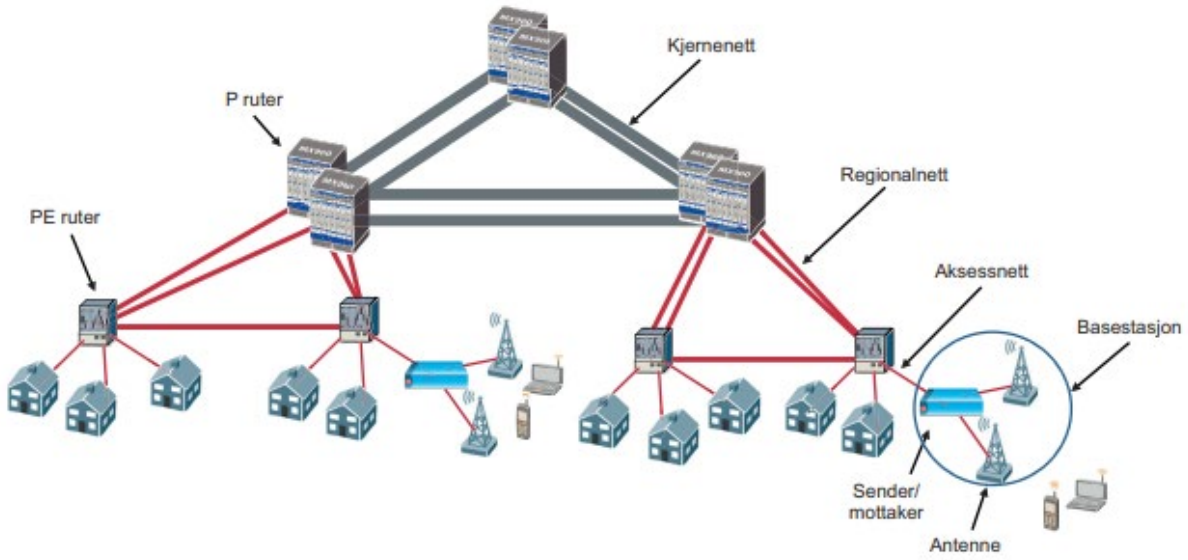
[71] NSM 2019 – Helhetlig digitalt risikobilde
[72] Regjeringen – Elektronisk kommunikasjon
[73] Nkom – Om Nkom
[74] Nkom drifter også Computer Emergency Response Team for ekomsektoren (EkomCERT) for håndtering av cyberhendelser.
[75] Ekomloven §2-10
[76] Ekomforskriften §8-2
[77] Nkom – Tilbyderes sikkerhets- og beredskapsplikter

kommunikasjonsnett til alle landets bedrifter og innbyggere. Telenor velger selv hvilken teknologi som skal ligge til grunn.[78] [79]

Justis- og beredskapsdepartementet har ansvaret for nødnett. Nødnett eies, driftes og forvaltes på deres vegne av Direktoratet for samfunnssikkerhet og beredskap (DSB). Nødnett tilbyr sikker kommunikasjon internt i, og på tvers av organisasjoner. Det benyttes av nødetatene, frivillige organisasjoner og en rekke andre offentlige og private aktører i samfunnet, herunder flere kommuner.[80]

Sårbarhet

Ekstremvær og alvorlige naturhendelser vil i fremtiden utsette infrastrukturen til ekom for større påkjenninger. Regional- og aksessnettene er i den sammenheng den mest sårbare delen av infrastrukturen til ekom[81].



Figur 15: Kilde: Oslo Economics, hentet i NOU 2015:13: Digital sårbarhet – sikkert samfunn

Linjebrudd vil i hovedsak være som en følge av en naturhendelse som f.eks. ekstremvær eller brann, men det kan også være så enkelt som en graveskade eller jordras. Et enkelt linjebrudd vil kunne føre til utfall eller begrenset kapasitet for ekom i et avgrenset

[78] Nkom - Abonnement
[79] Nkom – Telenor legger ned kobbernettet – hvilke rettigheter har du som forbruker?
[80] DSB – Hva er nødnett?
[81] Nkom – EkomROS 2021

geografisk område. Flere samtidige linjebrudd kan medføre bortfall eller begrenset kapasitet i et større område og noen ganger i hele regioner.

Ved teknisk feil skilles det mellom fysisk og logisk feil. En fysisk feil kan være overoppheting av komponenter som en følge av svikt i kjøling, feilmontering og skader på komponenter under vedlikehold. Logisk feil kan være feilkonfigurering eller feil i programvare som styrer trafikken eller produserer tjenester i nettet. Stadig flere funksjonaliteter i nettet har med programvare å gjøre, noe som igjen vil gjøre at logiske feil utgjør en stadig større andel av feilårsakene.

Uvanlig stor trafikk vil normalt oppstå når store folkemengder samler seg i et område. Dette kan være knyttet opp mot ulykker eller store hendelser som konserter eller festivaler. Bortfall av energiforsyning kan også medføre økt trafikk på de stasjonene som fortsatt er i drift.

Et langvarig bortfall av elektronisk kommunikasjon og strøm vil kunne påvirke mange samfunnskritiske funksjoner: At alt henger sammen med alt kommer tydelig frem ved hendelser knyttet til kritiske samfunnsfunksjoner og kritisk infrastruktur.

Forsterket ekom (FEKOM):

Agder har 12 kommuner med forsterket ekom. Det vil si at det er 72 timers nødstrøm for utvalgte basestasjoner i kommunene og hovedforbindelsene til basestasjonene, i tillegg til reserveforbindelse[82].

[82] Nkom – Har styrket elektronisk kommunikasjon ved kriser på indre Agder;
Nkom – Program for forsterket ekom

Figur 16: Oversikt over forsterkede basestasjoner i Agder.

Robusthet i kraft, ekom, informasjon og velferdsteknologi i Agder (KEIV) er et regionalt prosjekt i regi av Statsforvalteren, med formål om at relevante aktører sammen skal dele informasjon om sårbarheter, infrastruktur, vurderinger av hva som er kritisk infrastruktur og kritiske samfunnsfunksjoner (KIKS).[83] Prosjektet henger sammen med flere andre prosjekter i Agder for å styrke KIKS og samhandling.

[83] Meld.St. 29 (2020-2021) Vår felles digitale grunnmur – Mobil, bredbånd og internettjenester

Figur 17: Alt henger sammen med alt. Kraft og ekom er premissene for det digitale samfunnet, velferdsteknologien, deling av situasjonsbilder, men også for at kritisk infrastruktur og kritiske samfunnsfunksjoner skal fungere i fred, under kriser og i krig. Statsforvalteren i Agder har sammen relevante aktører flere prosjekter for å ivareta helheten på en best mulig måte.

Ekom er sektoroverskridende i den forstand at samfunnet vårt i veldig stor grad digitaliseres og avhengighetene av ekom øker. Det gjelder i stor grad for kritiske samfunnsfunksjoner. Stadig, og rask digital utvikling bidrar også til et mer uoversiktlig risiko- og sårbarhetsbilde, hvor nye sårbarheter oppstår og kan utnyttes av trusselaktører.[84]

I fylket finnes det alternative kommunikasjonssystemer hos kommuner og offentlige etater, slik som satellittelefoner, sikringsradioer, graderte nett og nødnett.

Erfaring fra kommuner viser at det har tatt opptil en uke før utfall og problemer har blitt feilrettet. For kommunene og regionale etater er det da viktig å kunne skape seg god situasjonsforståelse slik at feilretting kan foregå i en prioritert rekkefølge. Det finnes flere karttjenester som viser dekning og utfall. Blant annet har flere tilbydere en slik tjeneste for 2G, 4G og 5G[85].

Konsekvenser

[84] NSM – Risiko 2022

[85] Telenor - Dekningskart; Telia - Dekningskart; Områder med dekningsfeil; ICE - Dekningskart

Liv og helse

Manglende tilgang til medisinske journalsystemer, manglende mulighet eller forsinket varsling til nødetatene, og manglende kommunikasjon mellom operasjonssentralene og mannskaper kan få konsekvenser for liv og helse, herunder svikt i velferdsteknologi.

Samfunnsstabilitet

Utfall i mobiltjenester har stor påvirkning på befolkningens hverdag og trygghetsfølelse.

Usikkerhet

Avgrensede utfall forekommer i Agder inntil flere ganger i året. Det er sjeldnere at det forekommer omfattende og lengre utfall, men det foreligger historisk erfaring fra slike hendelser fra flere områder i Agder. I NSM sin årlige trusselvurdering kan man lese om internasjonale og nasjonale utsikter som også påvirker oss i Agder.

Størsteparten av rapportene og informasjonen som er lagt til grunn er hentet fra Nkom og andre dokumenter utarbeidet av offentlige aktører, herunder kommunenes helhetlige ROS-analyser. Det er også hentet innspill fra flere ekom-aktører. Det er ikke store avvik i informasjonen fra de ulike aktørene. Usikkerheten i kunnskapsgrunnlaget vurderes som liten.

Risikovurdering

Mulige risikoreduserende tiltak

- Gjennomføre jevnlige øvelser med bruk av alternativt samband.
- Tilgjengelig og oppdatert planverk for beredskap og opprettholdelse/gjenoppretting av tjenester ved utfall av ekom.
- Aktører i fylket bør benytte makten de besitter som bestillere av tjenester ved å fastsette krav til tilbydere av ekomtjenester om sikkerhet og tilgjengelighet, også i ekstraordinære situasjoner.
- Samarbeid mellom kraft, ekom og eiere av KIKS for å finne helhetlige og robuste løsninger.