Statsforvalteren i Nordland

Nordlaanten Staatehaaltoje
Nordlánda Ståhtaháldadiddje

Scenario 15: Flere nordlands-kommuner rammes av et cyberangrep

Sist oppdatert: 14.05.2024

Hendelsestype: Tilsiktet hendelse
Risikoområde: Cyberangrep
Scenario: Flere nordlands-kommuner rammes av et cyberangrep

Illustrasjonsbilde: Pixabay

Hendelsestype: Tilsiktet hendelse
Risikoområde: Cyberangrep
Scenario: Flere nordlands-kommuner rammes av et cyberangrep

Innledning

Dette avsnittet gir en innføring i risikoområdet, og en oversikt over de mest relevante hendelsene de siste årene.

Cyberangrep representerer en særskilt risiko for kritiske samfunnsfunksjoner på tvers av samfunnet. Samfunnets økte digitale avhengighet øker tilsvarende samfunnets sårbarhet for cyberangrep. Et cyberangrep er et angrep fra en ekstern eller intern trusselsaktør som har som hensikt å påføre en privatperson eller en virksomhet skade eller tap.[1] Det norske – og andre vestlige– samfunn har i mange år levd med cyberangrep rettet mot forskjellige etater og virksomheter, utført av ukjent aktører.

Dagens sikkerhetspolitiske situasjon utgjør en ytterlig risiko for cyberangrep. Begrep som sammensatte trusler og hybride angrep blir benyttet for å beskrive denne sikkerhetspolitiske situasjonen, og er elementer som påvirker forebyggingstiltak og krisehåndteringsevnen til eiere av kritiske samfunnsfunksjoner. I sin helhet er også Totalforsvaret utsatt for et endringsbehov for å kunne styrke sin robusthet. Disse elementene blir videre utdypet i scenarioet «sikkerhetspolitisk krise», og nevnes her for å understreke den sektorovergripende egenskapen til cyberangrep. I den sammenhengen kan cyberangrep utføres for å innhente sensitiv informasjon, både for å videreutvikle egen teknologi og for å avdekke sårbarheter.

I perioden 2017-2022 håndterte Statsforvalteren to hendelser tilknyttet cyberangrep.
I desember 2021 ble Nordlands Fylkeskommune utsatt for et omfattende dataangrep. Trusselsaktør hadde kommet seg på innsiden, og installert en programvare som utløste alarm i sikkerhetssystemene. I januar 2022 hadde håndteringen av hendelsen kostet Nordlands Fylkeskommune 11,7 millioner kroner.

I mars 2021 ble Øksnes kommune utsatt for et omfattende dataangrep. Ukjente aktører hadde kommet seg inn i Exchange-serveren gjennom en digital sårbarhet. Totalt kostet angrepet kommunen rundt 1 million kroner.

Fylkes-ROS 2019 har et scenario som het «vannforsyningssvikt etter cyberangrep». I årets omskriving av Fylkes-ROS er disse delt opp i to ulike scenario, slik at denne utgaven har et scenario for cyberangrep og et for vannforsyningssvikt. I Fylkes-2024 analyseres et scenario med et cyberangrep som rammer flere kommuner i Nordland.

I dette scenarioet analyseres sårbarheten og risikoen tilknyttet et cyberangrep som utfordrer en rekke kritiske samfunnsfunksjoner.

[1] Les «Cyberangrep – hva er det?», publisert online av *Telenor*. Hentet 07.08.2023.

Hendelsestype: Tilsiktet hendelse
Risikoområde: Cyberangrep
Scenario: Flere nordlands-kommuner rammes av et cyberangrep

Scenario

I tabellen beskrives hendelsesforløpet, og det gis en oversikt over resultatene av sårbarhets- og risikoanalysene.

Eksempel på hendelsesforløp	
På nyttårsaften blir det kjent at flere kommuner i Nordland er blitt rammet av et cyberangrep. Et sikkerhetshull i en felles programvare er blitt utnyttet, slik at hackerne har fått tilgang til flere kommuners interne servere. Programvaren blir benyttet av flere kommunale etater som rammer skole, hjemmetjeneste og sykehjem. Angrepet blir oppdaget av systemleverandøren, men det er usikkert hvor lenge den har vært der. Denne nulldagssårbarheten medfører at det er vanskelig å vite hvilken informasjon som er gått tapt allerede. Løsningen blir å umiddelbart stenge alle systemer og servere før potensielt mer lekkasje av informasjon. Det tar fem uker før serveren blir koblet på igjen. I denne tiden står rammete kommuner – med tilhørende kommunale tjenester – ovenfor en periode der tilgang til systemer er borte. Felles for alle nevnte kommunale etater er at vanlige kommunikasjonskanaler som er koblet til serveren, som e-post og chatfunksjoner, er lagt ned. Dette vanskeliggjør både intern og ekstern kommunikasjon på et generelt nivå. Det er usikkert hvem som står bak angrepet, og hvilken informasjon de klarte å innhente før systemene ble stengt. Dette bekymrer befolkningen i stor grad, og i kombinasjon med kommunikasjonsvansker er perioden preget av uro blant befolkningen. Befolkningen er spesielt bekymret over at sine egne sensitive personopplysninger muligens kan være på avveie hos en fremmed aktør. En rekke helsetjenester blir utfordret grunnet manglende tilgang til systemer. Hjemmetjenesten, sykehjem og legevakten mister sine vaktplaner, adresselister og kontaktinformasjon til pleietrengende, pasienter og pårørende. Dette vil gjøre det utfordrende for helseetatene å fullføre sine oppgaver ved å gi korrekt hjelp til rett tid. Hjelpe- og sykepleiere benytter vanligvis digitale plattformer for å innhente helseinformasjon til pasientene. Dette kan gjelde både hvilke type legemidler som skal benyttes og hvor mye doseringene ligger på. Svikt i disse systemene uten back-up løsning kan medføre blant annet feilmedisinering. Pårørende er svært bekymret over sine nærmeste som har behov for omsorg og pleie av kommunen. Når digitale opplysninger ikke er tilgjengelig vil det pådra seg økt ressursbruk innenfor både helsesektoren og andre tjenester i kommunen. Kommunens kriseledelse må prioritere sine ressurser med fokus på liv og helse. Det fordrer at de i kommunen er godt kjent med planverket, og har trent og øvet på lignende hendelser, slik at alle i krisestaben er klar over sine roller.	
Oversikt sårbarhetsanalyse	**Oversikt risikoanalyse**
1 kritisk samfunnsfunksjon vurdert som veldig sårbar (rød). 3 kritiske samfunnsfunksjoner vurdert som sårbar (gul). 5 kritiske samfunnsfunksjoner vurdert som lite sårbar (grønn).	Høy sannsynlighet med moderat usikkerhet. Store konsekvenser med moderat usikkerhet

Hendelsestype: Tilsiktet hendelse
Risikoområde: Cyberangrep
Scenario: Flere nordlands-kommuner rammes av et cyberangrep

Sårbarhetsanalyse

Sårbarhetsanalysen i Fylkes-ROS 2024 gjøres for å se på hvordan kritiske samfunnsfunksjoner påvirkes av den aktuelle hendelsen. Det gjøres en enkel analyse av sårbarheter (svakheter) innenfor den enkelte samfunnsfunksjonen som blir berørt.

Vi har valgt å benytte tre grader av sårbarhet: grønn (liten sårbarhet), gul (moderat sårbarhet) og rød (stor sårbarhet). Samfunnsfunksjoner med gul eller rød vurdering blir utdypet i delkapittelet «vurdering av kritiske samfunnsfunksjoner».

Samlet sårbarhetsanalyse

Tabellen nedenfor gir en presentasjon av resultatene fra sårbarhetsanalysen.

Kritisk samfunnsfunksjon	Sårbarhet
Forsyningssikkerhet	
Kraftforsyning	
Elektronisk kommunikasjon (EKOM)	
Transport	
Vannforsyning og avløp	
Helse- og omsorgstjenester	
Redningstjenester	
Styring og kriseledelse	
Husly og varme	

Vurdering av kritiske samfunnsfunksjoner

Scenarioets vurdering av kritiske samfunnsfunksjoner ble drøftet i møter mellom arbeidsgruppen og eiere av de utvalgte kritiske samfunnsfunksjonene.

Forsyningssikkerhet

Handlingene for å begrense skadene av cyberangrepet fører til at forsyningssikkerhet blir sårbar. Kommuner vil kunne verken sende faktura, gjennomføre betaling, eller overføre lønn til sine ansatte mens serveren er brutt. Bestilling av varer vil opphøre frem til nødløsninger er innført. Dette inkluderer viktige varer som for medisiner.

Forsyningssikkerhet er vurdert som sårbar (gul) fordi en rekke varer som er nødvendig for driften av kommunale tjenester ikke vil kunne bestilles før alternative løsninger er innført.

Elektronisk kommunikasjon (EKOM)

Handlingene for å begrense skadene av cyberangrepet fører til at EKOM blir sterkt påvirket. Fasttelefon og mobiltelefoner for ansatte antas å enda fungere. Mange telefonløsninger i resepsjoner er koblet opp mot nettet, og det er derfor forventet at en del av kommunikasjonen vil falle ut for disse tjenestene. Øvrige digitale tjenester og meldingssystemer vil også falle ut fordi tjenestene er frakoblet internettet.

EKOM er vurdert som sårbar (gul) da den beste løsningen ved oppdagete cyberangrep er å stenge EKOM-tjenester for å unngå spredning og tap av informasjon. Dette fører til at kommunen må finne andre måter å kommunisere på. Ved å sette opp andre serverløsninger kan kommunen gjenopprette intern kommunikasjon.

Helse- og omsorgstjenester

En rekke helsetjenester blir utfordret grunnet manglende tilgang til systemer. Hjemmetjenesten, sykehjem og legevakten mister sine vaktplaner, adresselister og kontaktinformasjon til pleietrengende, pasienter og pårørende. Dette vil gjøre det utfordrende for helseetatene å fullføre sine oppgaver ved å gi korrekt hjelp til rett tid. Hjelpe- og sykepleiere benytter vanligvis digitale plattformer for å innhente helseinformasjon til pasientene. Dette kan gjelde både hvilke type legemidler som skal benyttes og hvor mye doseringene ligger på. Svikt i disse systemene uten back-up løsning kan medføre blant annet feilmedisinering. Pårørende er svært bekymret over sine nærmeste som har behov for omsorg og pleie av kommunen.

Helse- og omsorgstjenester er vurdert som veldig sårbar (rød). Den daglige driften av en rekke helsetjenester blir sterkt påvirket, og krever mye innsats og ressurser for å unngå alvorlige følgekonsekvenser.

Styring og kriseledelse

På lokalt nivå

Når digitale opplysninger ikke er tilgjengelig vil det pådra seg økt ressursbruk innenfor både helsesektoren og andre tjenester i kommunen. Kommunen får ikke kjørt utbetalinger til sine borgere, det kan påregnes stengte skoler grunnet manglende timeplaner og klasseoversikter, og helsesektoren vil oppleve en rekke utfordringer for å gi sine pasienter livskritisk oppfølging og behandling.

Kommunens kriseledelse må prioritere sine ressurser med fokus på liv og helse. Det fordrer at de i kommunen er godt kjent med planverket, og har trent og øvet på lignende hendelser, slik at alle i krisestaben er klar over sine roller. Kommuner som mangler fysiske kopier av lister (eksempelvis kontaktlister), planer (eksempelvis beredskapsplaner), og dokumenter (eksempelvis tiltakskort) er fortsatt nødt til å innkalle medlemmer av krisestab til møte, henvende seg til beredskapsplanen og følge punktene fastsatt i tiltakskortene.

Et cyberangrep vil utfordre kommunens styring og kriseledelse ved at kommunen må sette inn ressurser på helseområdet, og omprioritere andre oppgaver i denne fasen.

På regionalt nivå

Statsforvalteren vil som del av sin samordningsrolle være kontaktpunktet mellom sentrale myndigheter og kommunen og vil ha et ansvar for å sørge for informasjonsflyt fra sentralt hold til kommunene og motsatt vei.

På nasjonalt nivå

Ut fra det store omfanget, vil denne hendelsen være å oppfatte som en nasjonal krisehendelse, særlig i mediesammenheng.

Samlet vurdering av styring og kriseledelse

Styring og kriseledelse er vurdert som veldig sårbar (rød) fordi den ordinære driften til kommunen blir påvirket, med behov for god informasjonsinnhenting og -formidling. Det vil være behov for god koordinering og samarbeid på tvers av myndighetsnivåene for å samordne krisehåndteringen, noe som kan bli ytterlig utfordret grunnet den sammensatte trusselen på flere samfunnsnivåer. Hendelsen vil vekke stor nasjonal og muligens internasjonal oppmerksomhet.

Hendelsestype: Tilsiktet hendelse
Risikoområde: Cyberangrep
Scenario: Flere nordlands-kommuner rammes av et cyberangrep

Risikoanalyse

Scenarioet «flere kommuner rammes av et cyberangrep» er et eksempel på hvordan en hendelse innenfor risikoområdet «cyberangrep» kan utvikle seg. Lokale forskjeller i geografi, infrastruktur og demografi vil utgjøre forskjeller i samfunnets robusthet (mer om dette i delkapittelet «overførbarhet») ved en slik hendelse.

Vi har valgt å bruke fem nivåer i vurdering av sannsynlighet (svært lav til svært høy) og konsekvenser (fra svært liten til svært store), og tre nivåer i vurdering av usikkerhet (små, moderat og stor). Begrunnelsen for vurderingene utdypes videre i delkapitlene «vurdering av sannsynlighet», «vurdering av konsekvenser» og «vurdering av usikkerhet».

Samlet risikoanalyse

Tabellen nedenfor gir en presentasjon av resultatene fra risikoanalysen.

Sannsynlighetsvurdering						
	Svært lav	**Lav**	**Moderat**	**Høy**	**Svært høy**	**Forklaring**
Sannsynligheten for at hendelsen skal inntreffe er 1%						Antas å kunne skje en gang i løpet av 100 år.

Konsekvensvurdering							
Verdi	**Konsekvenstype**	**Svært liten**	**Liten**	**Moderat**	**Store**	**Svært store**	**Forklaring**
Liv og helse	**Dødsfall**						To dødsfall.
	Skader og sykdom						Seks registrerte personskader.
Stabilitet	**Påkjenninger i hverdagen**						Befolkningen i flere kommuner rammes i fem uker.
	Sosial og psykologiske påkjenninger						Fem av seks kjennetegn til stede i moderat til stor grad.
Natur og kultur	**Skader på naturmiljø**						Ingen registrerte skader.
	Skader på kulturminner og -miljø						Ingen registrerte skader.
Økonomi	**Direkte og indirekte kostnader**						50-150 millioner kroner.
Samlet vurdering av konsekvenser							Totalt sett store konsekvenser.

Usikkerhet	**Liten**	**Moderat**	**Stor**

Vurdering av sannsynlighet

Scenarioets sannsynlighetsvurdering bygges på sammenlignbare hendelser, lokale forutsetninger og offentlige rapporter/dokumenter.

Blant de mange eksemplene av cyberangrep i Norge er angrepet på Nordlands Fylkeskommune og Øksnes kommune i 2021, som ble nevnt i innledningen. Et annet eksempel er fra mai 2022, da det ble kjent at en kopi av Norges offisielle eiendomsregister hos karttjenesten Norkart – som henter data fra Statens kraftverk – var lekket til en ukjent trusselsaktør. Persondata om 3,3 millioner nordmenn hvor navn, adresser, fødselsnummer og informasjon om hva man eier på avveie.[2] Et til eksempel er fra januar 2021, da hackere tok seg inn bak brannmuren til Østre Toten kommune, slettet alle sikkerhetskopier, krypterte alle data, og la ut sensitiv informasjon på det mørke nett. I september 2021 sto den totale kostnaden av angrepet på 30 millioner kroner.[3]

Ifølge NSM har alvorlige cyberoperasjoner mot norske myndigheter og virksomheter tredoblet seg fra 2019 til 2021. Distribuerte tjenestenektangrep, phishing og kartleggingsaktivitet var blant de vanligste angrepsmetodene. Sikkerhetsnivå og -status kan fortsatt forbedres i mange norske virksomheter, og NSM ser stadig utnyttelse av menneskelige, teknologiske og organisatoriske sårbarheter for å understøtte ondsinnede cyberoperasjoner. [4] NSM påpeker at: «det vil også være aktivitet i cyberdomenet som ikke avdekkes, og det er derfor viktig å understreke at fravær av bevis på aktivitet ikke er det samme som bevis på fravær.» [5]

I senere år er enkeltpersoner blitt mer utsatt for cyberangrep. Dette inkludere politiske beslutningstagere, forskere, militært personell, dissidenter og diaspormiljøer som blir utsatt for angrep fra fremmede etaters etterretningstjenester. Den generelle dårlige IKT-sikkerheten blant privatpersoner og virksomheter forsterke risikoen til cyberangrep.[6]

I scenarioet «flere kommuner rammes av et cyberangrep» vurderes sannsynligheten for at hendelsen inntreffer som høy (1 gang i løpet av 100 år).

[2] Les «Risiko 2023: økt forutsigbarhet krever høyere beredskap», publisert av *NSM* online 13.02.2023. Side 18.
[3] Les A.M.s «Når krisen kommer», publisert av *NRK* online 01.09.2021.
[4] Les «Risiko 2023: økt forutsigbarhet krever høyere beredskap», publisert av *NSM* online 13.02.2023. Side 18.
[5] Les «Risiko 2023: økt forutsigbarhet krever høyere beredskap», publisert av *NSM* online 13.02.2023. Side 18.
[6] Les «Nasjonal trusselvurdering 2023», publisert av *PST*. Hentet 15.08.2023. Side 16.

Vurdering av konsekvenser

Scenarioets konsekvensvurdering bygges på resultatene fra sårbarhetsanalysen og drøftinger med interne og eksterne parter. Vurderingene beskriver først mulige faktorer innenfor risikoområdet som kan påvirke alvorlighetsgraden. Deretter vurderes konsekvensen spesifikt innenfor det utvalgte hendelsesforløpet.

Liv og helse

Konsekvensen et cyberangrep har på liv og helse er avhengig av hvilken virksomhet som rammes, og om angrepet blir oppdaget. Eventuelle konsekvenser til liv og helse skyldes med sannsynligvis indirekte følger, og ikke direkte følger, av at cyberangrepet blir oppdaget og dermed medfører stenging av server og internettilgang.

Konsekvensene cyberangrep på liv og helse ifølge hendelsesforløpet

Konsekvensene av «flere nordlands-kommuner rammes av et cyberangrep» vurderes å være liten for liv og moderat helse. Dette skyldes at kommunen – og tilhørende kommunale tjenester – mister tilgang til viktige dokumenter og rutiner, som for eksempel prioriteringsliste for hjemmeboende. I tillegg kan helse- og pleiehjelp, samt barnevernet, ikke motta bekymringsmeldinger, og ordningene mister tilgang til sine journaler. Alle sektorer tilknyttet kommunen som bruker den samme programvaren mister oversikt.

Det antas at manglende og/eller forsinket oppfølging av de som har hjemmepleiehjelp fører til at to mennesker mister livet.

Det antas også at seks mennesker får manglende og/eller forsinket oppfølging av de som har hjemmepleiehjelp og andre kommunale støtteordninger. Dette inkluderer et barn som blir alvorlig skadd av en foresatt, til tross for forsøk av nærstående å sende inn bekymringsmelding til barnevernet.

Stabilitet

Konsekvensvurderingen av stabilitet bygges på to elementer. Det første er «påkjenninger i hverdagen», som handler om de negative konsekvensene bortfall av kritiske samfunnsfunksjoner har på samfunnet i forbindelse med en hendelse. Det andre elementet er «sosiale og psykologiske påkjenninger», som handler om følelsesmessige reaksjoner blant befolkingen i forbindelse med en hendelse. Stabilitet, og hvordan konsekvensen vurderes, er utdypet ytterlig i sammendraget.

Eventuelle konsekvenser til stabilitet kan skyldes direkte følger av cyberangrepet som ikke blir oppdaget umiddelbart, som for eksempel dersom formålet med angrepet er å spre desinformasjon. Konsekvensene kan også skyldes indirekte følger av cyberangrepet, dersom det blir oppdaget, og dermed medfører stenging av servere og internettilgang.

Ansatte og kunder i en rammet virksomhet vil merke endringer i den daglige driften. Avhengig av hvilken virksomhet som rammes, så kan et cyberangrep medføre «påkjenninger i hverdagen». Dette gjelder for virksomheter med ansvar for kritiske samfunnsfunksjoner. Avhengig av virksomhetens betydning og rolle i samfunnet, kan flere oppleve følgekonsekvensene.

Følgende «sosiale og psykologiske påkjenninger» forventes å belaste samfunnet ved en sikkerhetspolitisk krise:

- Rammer sårbare grupper spesielt
- Tilsiktet hendelse

Hendelsestype: Tilsiktet hendelse
Risikoområde: Cyberangrep
Scenario: Flere nordlands-kommuner rammes av et cyberangrep

- Manglende mulighet til å unnslippe
- Forventingsbrudd
- Manglende mulighet til å håndtere hendelse

Konsekvensene av cyberangrep på stabilitet ifølge hendelsesforløpet

Konsekvensene av «flere nordlands-kommuner rammes av et cyberangrep» vurderes å være store for «påkjenninger i hverdagen» og store for «sosiale og psykologiske påkjenninger». Det antas at scenarioet innebærer «påkjenninger i hverdagen» for alle innbyggerne i det utsatte området. En rekke livsviktige varer og tjenester faller bort over lengre tid grunnet sammenfallet av kraftforsyningssvikt og uvær.

Det antas at scenarioet inneholder fem av de seks definerte kjennetegnene som kan indikere «sosiale og psykologiske påkjenninger».

Følgekonsekvensene av tiltakene mot et gjennomført cyberangrep – det vil si stenging av serveren – medfører at myndighetene jobber saktere eller ikke kan utføre oppgavene sine i det hele tatt. Dermed rammes de **mest sårbare grupper spesielt**, noe som vil føre til store følelsesmessige reaksjoner dersom noen – som i dette tilfelle – omkommer grunnet manglende kommunal oppfølging.

Cyberangrepet er planlagt, og de rammete er utvalgt. Denne **tilsiktede hendelsen** vil medføre moderat bekymringer og frykt for arbeidstakere med lignende kompetanse og tilgang.

Hendelsen medfører **manglende mulighet til å unnslippe** fordi valgene tatt for å unnslippe konsekvensene av cyberangrepet medfører at en rekke EKOM-tjenester knyttet til kommunal virksomhet faller ut. Dette utfallet overlate berørte til en rekke følgekonsekvenser som ikke er mulig å unnslippe, noe som i stor grad medfører fører til følelser om avmakt og usikkerhet. Blant disse følgekonsekvensene er «manglende mulighet til å håndtere hendelsen». Cyberangrepet vil føre til **forventingsbrudd** overfor myndigheten, og vil bidra til en stor grad av kritikk og mistillit overfor ansvarlige myndigheter og leverandører av kritiske samfunnsfunksjoner.

Følgekonsekvensene av tiltaket for å begrense skadeomfanget skaper en **manglende mulighet til å håndtere hendelsen**. Dette vil føre til en stor grad av redsel, usikkerhet og avmakt blant befolkningen.

Hendelsestype: Tilsiktet hendelse
Risikoområde: Cyberangrep
Scenario: Flere nordlands-kommuner rammes av et cyberangrep

Økonomi

Et cyberangrep medfører direkte økonomiske tap knyttet til gjenoppretting av feilen. Det indirekte økonomiske tapet omfatter merkostnader og tapte inntekter for rammet virksomhet. For kommunene vil merarbeidet innenfor tjenesteområdet innebære store ekstrakostnader. Ikke minst kan et cyberangrep medføre både et stort omdømmetap og store bøter for den rammete virksomheten.

Konsekvensene av cyberangrep på økonomi ifølge hendelsesforløpet

Konsekvensene av «flere nordlands-kommuner rammes av et cyberangrep» vurderes å være moderat for økonomi. Det antas et samlet økonomisk tap på rundt 50-150 millioner kroner. I tillegg opplever de rammete kommunene sterk kritikk for cyberangrepet, og dermed omdømmetap.

Det direkte økonomiske tapet knyttes til gjennomføring av nødvendige tiltak for å gjenopprette en trygg servertilkobling, og antas å beløp seg til flere titalls millioner.
Det indirekte økonomiske tapet som følge av tapt fortjeneste antas å beløpe seg til under 10 millioner.

Vurdering av usikkerhet

Scenarioets usikkerhetsvurdering bygges subjektive refleksjoner over kunnskapsgrunnlaget tilgjengelig under revisjonen av Fylkes-ROS 2024.

I tabellen presenteres usikkerhetsvurderingen.

Kunnskapsgrunnlaget	Merknad
Tilgang på relevante data og erfaringer	Relevant data og erfaring tilknyttet risikoområdet er tilgjengelige og pålitelige.
Forståelse av hendelsen som analyseres (hvor kjent og utforsket er fenomenet)	Risikoområdet er kjent. Risikoområdet er derimot ikke enkel å forstå, spesielt med tanke på leveringssystemet og antall underleverandører til ulike IKT-tjenester.
Samlet vurdering av usikkerhet	Usikkerheten tilknyttet sannsynlighetsvurderingen vurderes som moderat. Usikkerheten tilknyttet konsekvensvurderingen vurderes som moderat.

Overførbarhet

Avsnittet beskriver hvordan sårbarheten og risikoen skissert i dette scenarioet kan påvirkes av ulike faktorer og detaljer.

Dette scenarioet er en uønsket hendelse som er **relevant for alle deler av Nordland** i mer eller mindre grad. Digitale tjenester og IKT-avhengighet på tvers av alle sektorer gjør samfunnet sårbar for mulige cyberangrep.

En viktig faktor som påvirker hendelsesforløpet til dette scenarioet, er **om cyberangrepet blir oppdaget eller ikke**, og også hvor raskt det blir oppdaget.

En grunnleggende **god IKT-sikkerhet** blant ansatte i en virksomhet er et viktig element som kan påvirke hendelsesforløpet til et mulig cyberangrep.

Tilgang til dokumenter som rutiner, vaktplaner og prioriteringslister er avgjørende for hvorvidt en virksomhet klarer å drifte uten tilgang til serveren. Harde kopier – eller digitale kopier på enheter som ikke er tilknyttet serveren – er mulige løsninger på dette, og faller innenfor en god IKT-sikkerhet. Norge er ikke direkte involvert i krigen i Ukraina, men den økte spenningen mellom NATO – der Norge er medlemsstat – og Russland medfører at det norske samfunnets sårbarhet ovenfor digitale trusler påvirkes direkte av den pågående geopolitiske krisen. Et utført cyberangrep risikerer å utfordre befolkningens tillit, og i **en sikkerhetspolitisk situasjon** står den politiske og demokratiske stabiliteten også på spill.

Klimaendringer

Klimaendringer er en global utfordring som vil få konsekvenser for sannsynligheten, konsekvensen, omfanget og forløpet av hendelser i det regionale sikkerhetsbilde. Vi har som overordnet mål å i større grad vurdere hvordan klimaendringer vil påvirke det regionale sikkerhetsbilde. I dette avsnittet redegjør vi preliminære tanker på hvordan scenarioet og/eller risikoområdet påvirkes av klimaendringene.

Klimaendringene kan påvirke cybersikkerheten på flere indirekte måter.

Hyppigere forekomst av smittsomme sykdommer, som krever raske og drastiske tiltak, kan påvirke den enkelte arbeidstakernes IKT-sårbarhet. COVID-19, og medfølgende hjemmekontor tilpasninger, medførte en viss risiko for IKT-sikkerheten. Digitale angrep i forkant eller under ekstrembærhendelser – som vil skje hyppigere og kraftigere enn før – kan føre til at flere kritiske samfunnsfunksjoner blir sårbare.

En annen måte klimaendringer kan påvirke cybersikkerhet er at teknologien som utvikles for å enten motvirke økt og kraftig forekomst av naturhendelser, eller for å motvirke klimaendringene er attraktive for fremmede aktører. Historisk sett er det stor konkurranse for teknologisk utvikling, og i en tid der sammensatte trusler og hybride angrep er økende risikoområder, så er det ikke utenkelig at teknologiske utviklinger i forbindelse med klimaendringer er ettertraktet informasjon. Dette gjelder også individer som jobber med klimaspørsmål.

Klimaendringenes omfang og alvor tilsier at vi er nødt til å tilpasse oss et endret klima, parallelt med at utslipp av klimagasser må reduseres kraftig, både i Norge og globalt. Vi må omstille oss til å bli et lavutslippssamfunn som også er klimarobust.[7]

Gjennom FN's bærekraftsmål har Norge forpliktet seg til å stoppe klimaendringene.[8] Hele spekteret, fra regjering til enkeltindividet, skal være med på omstillingsprosessen. Å iverksette nasjonale mål og tiltak er like viktig for regjering, som det for næringsliv og landets innbyggere. Våre vaner og forbrukertrender må også endres hvis vi skal lykkes med omstilling til å bli et lavutslippssamfunn. Ansvaret for omstilling til å bli et lavutslippssamfunn er altså fordelt på tvers av samfunnet.

Å gjøre IKT-sikkerhet mer klimarobust innebærer både å styrke selve IKT-sikkerhetskulturen, og å utarbeide gode planer i tilfelle man likevel blir rammet av et cyberangrep svikter. Relevansen for en mer robust IKT-sikkerhet øker med samfunnets voksende avhengighet på en digitalisert hverdag. Flere kommuner som rammes av et cyberangrep er vurdert som er scenario med høy sannsynlighet for å inntreffe. Klimaendringene forverre risikoen tilknyttet scenarioet.

[7] Les «Stortingsmelding 26» (2022-2023), publisert av *Regjeringen* 16.06.2023. Side 5.
[8] Les «Bærekraftsmålene», publisert på *Regjeringens* nettside. Hentet 24.11.2023.

Forebygging og beredskap

Dette avsnittet presenterer hvordan forebyggings- og beredskapsarbeid innenfor risikoområdet kan gjennomføres.

Mange kritiske infrastrukturer i dag er avhengige av EKOM-tilgang og digitale tjenester. Automatiske brannvarslere, innbruddsalarmer, trygghetsalarmer, samt drift av kritisk infrastruktur som vei, vann, avløp og strøm er alle koblet på nett. Dette medfører sårbarhet for cyberangrep.

Forebygging- og beredskapsarbeidet i cyberangrepssammenheng omfatter i hovedsak to elementer: en god, intern IKT-sikkerhetskultur som minimere sjansen for å bli utsatt av et cyberangrep, og en strategisk plan dersom et cyberangrep likevel skulle kunne inntreffe. Eksempler på god IKT-sikkerhetskultur inkluderer interne seminarer på gode vaner. Eksempler på strategisk plan inkluderer alternative kommunikasjonssystemer med aktuelle parter.

Dagens sikkerhetspolitiske situasjon utfordrer forståelsen av Totalforsvaret, ved å sette spørsmålstegn bak hvordan Totalforsvaret kan sikre seg mot cyberangrep. Enkeltpersoner utgjør en del av Totalforsvaret, og da er det ikke tilstrekkelig for en bedrift å ha gode IKT-sikkerhetskultur og strategiske plan i tilfelle av et cyberangrep. Individet må også forstå hvor viktig det er å være forberedt på mulige cyberangrep.

Videre påpeker dagens sikkerhetspolitiske situasjon at tilfeller som for eksempel cyberangrep utgjør en del av et mye større bilde – nemlig hybride angrep og sammensatte trusler. Det omhandler ikke lenger kun at fremmede aktører ønsker tilgang til data for enten penger eller informasjon, men det er suvereniteten til nasjonalstater som står på spill.