1. Generelt om tilsynene

I desember 2016 ble hendelsen som refereres til som «Nødnett-saken» kjent. Saken satte fokus på tjenesteutsetting til utlandet. På bakgrunn av hendelsen og opplysninger i media om at Nødnett kunne påvirkes negativt, opprettet Nasjonal sikkerhetsmyndighet (NSM) tilsynssaker med Direktoratet for nødkommunikasjon og Motorola Solutions Norway AS (Motorola), som er hovedleverandør for Nødnett. Fra 1. mars 2017 overtok Direktoratet for samfunnssikkerhet og beredskap (DSB) ansvaret for Nødnett, og tilsynet fortsatte derfor med DSB som tilsynsobjekt. Nasjonal kommunikasjonsmyndighet (Nkom) opprettet tilsynssak med Broadnet AS. Tilsynsmyndighetene NSM og Nkom hadde tett dialog og deltok i hverandres stedlige tilsyn for å sikre helhetsoversikt i saken. I tillegg iverksatte Politiets sikkerhetstjeneste (PST) etterforskning.

Motorola avdekket i desember 2016 uautorisert tilgang til deler av Broadnets systemer fra driftspersonell hos Tech Mahindra i India. Hendelsen ble etter en tid rapportert til NSM og Nkom. Forholdet ble omtalt i media som «Nødnett-saken». Nødnett-avtalen er organisert slik at Motorola som hovedleverandør har tilnærmet et totalansvar for drift av Nødnett. Motorola er et globalt selskap som i forbindelse med drift av Nødnett har valgt å benytte sentraliserte spisskompetansemiljøer i utlandet.

Broadnet AS leverer en betydelig del av den underliggende infrastrukturen (transmisjonsnett, dekker ca. 40 % av befolkningen) som benyttes for kommunikasjon i Nødnett. Broadnet valgte høsten 2015 å tjenesteutsette deler av sin IT- og nettverksdrift til teknologiselskapet Tech Mahindra Limited. Avtalen innebar at deler av arbeidsoppgavene kunne bli tjenesteutsatt til Tech Mahindra i India. Nkom ga Broadnet veiledning i prosessen med tjenesteutsetting. På bakgrunn av denne veiledningen ble den planlagte tjenesteutsettingen endret, slik at deler av driften ble værende i Norge. Tilsynet med Broadnet har imidlertid avdekket at Broadnet ikke har fulgt opp veiledningen videre i prosessen med tjenesteutsetting til India.

Deler av infrastrukturen som utgjør Nødnett og deler av Broadnets landsdekkende transmisjonsnett er på grunn av sin samfunnskritiske funksjon utpekt som skjermingsverdige objekter i henhold til sikkerhetsloven. Eksempler på skjermingsverdige objekter i forbindelse med de omtalte tilsynssakene er sentral IKT-infrastruktur med tilhørende styringssystemer.

Objekter som er utpekt som skjermingsverdige er gjennom lov og forskrift underlagt krav til særskilte sikringstiltak. Ett slikt tiltak er at det kan stilles krav til at personell med permanent tilgang til skjermingsverdige objekter skal være sikkerhetsklarert og/eller autorisert. Sektordepartementene har stilt krav til sikkerhetsklarering og/eller autorisasjon for personell med permanent tilgang av fysisk art eller logisk art (elektronisk tilgang til IKT-systemer) til skjermingsverdige objekter i Nødnett og hos Broadnet.

Regimet rundt krav til beskyttelsestiltak for skjermingsverdige objekter og tilsyn med etterlevelse av disse er organisert slik at der det finnes et dekkende sektorregelverk og en tilsynsmyndighet som fører kontroll med etterlevelse av dette regelverket, vil dette primært være det regelverket som kommer til anvendelse for skjermingsverdige objekter i den aktuelle sektor. På bakgrunn av dette sektorprinsippet førte Nkom tilsyn med Broadnet i henhold til ekomlovens bestemmelser, herunder hvordan de funksjonelle kravene i objektsikkerhetsforskriften oppfylles, mens NSM førte tilsyn med DNK og Motorola i henhold til sikkerhetslovens bestemmelser.

Nkom har ført tilsyn med forhold knyttet til hendelsen og for å avdekke bakenforliggende årsaker. Gjennom Nkoms tilsyn med Broadnet framkom det at selskapet hadde tildelt personell hos Tech Mahindra i India systemtilganger til styringssystemer de ikke skulle hatt. De urettmessige tilgangene viste seg å være mer omfattende enn kun å angå Nødnett. Nødnett var derfor ikke den eneste kunden som kunne påvirkes fra India.

NSM har ved tilsynene foretatt undersøkelser i et noe bredere perspektiv enn den rapporterte hendelsen, for å undersøke hvordan sikkerhetsstyring og forebyggende sikringstiltak for skjermingsverdige objekter har blitt fulgt opp av DSB og Motorola.

NSM og Nkom vil presisere at tilsynene ikke har omfattet en fullstendig gjennomgang av alle forhold knyttet til forebyggende sikkerhet, herunder objektsikring hos tilsynsobjektene. Tilsynene har avdekket omfattende og alvorlige sårbarheter som det har vært nødvendig å følge opp.

2. Tjenesteutsetting

De senere årene har det både i Norge og i en rekke andre land, vært et økende omfang av utsetting (konkurranseutsetting/ utkontraktering) av IKT-tjenester, herunder også til utlandet. Bakgrunnen for tjenesteutsettingen er ofte økonomisk motivert. Eksempelvis vil visse typer IKT-tjenester kunne leveres rimeligere blant annet via fjerndrift fra lavkostland. Videre ser vi også at det benyttes sentraliserte spisskompetansemiljøer f.eks. i utlandet, framfor å bygge opp kompetanse nasjonalt.

Utsetting av tjenester er i seg selv ikke negativt. Viktige forutsetninger for å få til en vellykket tjenesteutsetting er å ha kontroll på egne verdier, kjenne egne sårbarheter og trusselbildet før man starter prosessen. Tjenesteutsetting kan blant annet gi bedre tilgang til kompetanse, større skalerbarhet og spare virksomheten for utgifter, men det er nødvendig å investere i både tekniske, administrative og organisatoriske sikkerhetstiltak i egen virksomhet for å kompensere for den økte sårbarheten. Ansvaret for sikkerheten kan således ikke settes ut.

Tjenesteutsetting av funksjoner som skal støtte opp under vitale nasjonale sikkerhetsinteresser – eksempelvis Nødnett, vil være mer krevende når det gjelder risikovurderinger, sikkerhets- og kontrolltiltak. Det er behov for en nærmere avklaring av om slike funksjoner bør være under tydeligere nasjonal kontroll og hvordan.

Ved vurdering av hvorvidt oppgaver og tjenester skal utsettes til eksterne, må det gjennomføres en risikovurdering, herunder for å avdekke lov- og forskriftskrav som må ivaretas, hvilken risiko man løper for egen virksomhet og kunder osv. Ulemper og behovet for

kompenserende tiltak som f.eks. ulike kontrollmekanismer, må veies mot fordeler. Videre må virksomheten fortsatt besitte ressurser til forvaltning av tjenesteutsettingen, herunder bestiller- og kontrollkompetanse. Gode og presise avtaler må inngås ved tjenesteutsetting, samt at oppfølging og faktiske kontroller av leverandører må foretas jevnlig og planmessig. Ved tjenesteutsetting og delegering vil det alltid være en fare for at det oppstår uklarheter med hensyn til ansvar, roller og oppgaver. Gode avtaler som bidrar til at partene har lik fortolkning kan imidlertid avhjelpe dette noe.

En fellesnevner ved de tre tilsynene er at deler av driften er tjenesteutsatt.

3. Funn

Nedenfor beskrives hovedtrekk fra tilsynene. Det gjøres oppmerksom på at de tre tilsynsrapportene er sikkerhetsgradert, og at alle detaljer i tilsynssakene derfor ikke kan gjengis.

Felles for tilsynene var at det framkom utfordringer og sårbarheter i forbindelse med utsetting av viktige tjenester tilknyttet skjermingsverdige objekter hvor personell uten norsk statsborgerskap i inn- og utland ble benyttet i stor utstrekning.

Tilsynene avdekket at virksomhetene hadde gjennomført enkelte tiltak for å styrke sikkerheten. Tiltakene var imidlertid ikke basert på en helhetlig, relevant risiko- og sårbarhetsvurdering, men fremstod som fragmentert og noe tilfeldig.

3.1 Fjerntilgang

Det ble ved tilsynene med Nødnett avdekket at personell fra utlandet hadde fjerntilgang til skjermingsverdige objekter uten at tilstrekkelige sikringstiltak var på plass. Det var ikke etablert tilstrekkelige barrierer og deteksjonsmuligheter i tilknytning til fjerntilgang. Virksomhetene hadde valgt å legge svakere krav til grunn for fjerntilgang (logisk tilgang) enn til fysisk adgang. Regelverket må anvendes på samme måte for logisk tilgang som for fysisk adgang. Det kan ikke stilles svakere krav til logisk sikring enn til fysisk sikring, ettersom skadepotensialet er vel så stort ved objekter hvor tilgangen er av logisk art.

Det ble ved tilsynene med Broadnet avdekket at personell i utlandet hadde fjerntilgang til skjermingsverdige objekter uten at tilstrekkelige sikringstiltak var på plass. På bakgrunn av dette kunne utenlandske statsborgere ved hjelp av fjernpålogging fra utlandet potensielt sette deler av Broadnets transmisjonsnett ut av drift, herunder leveranser til Nødnett.

Konseptet for drifts- og supporttjenester for Nødnett er utformet slik at det benyttes fjerntilgang til de skjermingsverdige objektene for tilgang til spisskompetanse lokalisert i utlandet. På bakgrunn av dette kunne eksempelvis fjernpålogget personell fra utlandet potensielt sette Nødnett ut av drift.

3.2 Logging

Ved alle de tre tilsynene kom det fram at tilsynsobjektene hadde mangelfulle logger fra systemene, og mangelfulle muligheter for å analysere disse. Eksempelvis ble ikke fjerntilgang til alle relevante systemer automatisk loggført. Det var derfor ikke mulig å detektere hvorvidt personell som hadde vært fjernpålogget, hadde utført illegitime handlinger.

3.3 Verdi- og risikovurdering

Kontinuerlig verdivurdering er en grunnleggende forutsetning for å identifisere hva som må beskyttes og med hvilke tiltak. Eksempelvis kan endrede krav i forbindelse med implementering av nytt objektsikkerhetsregelverk og utpeking av deler av infrastrukturen i Nødnett som skjermingsverdige objekter, medføre behov for forhøyet graderingsnivå på informasjon. Det er derfor viktig å gjennomføre kontinuerlig verdivurdering i et så langvarig prosjekt som Nødnett-prosjektet, fordi forholdene endrer seg underveis.

NSMs oppfatning er at det for Nødnett ikke har vært tilstrekkelig fokus i forbindelse med verdivurdering av informasjon, noe som kan ha medført at ikke all skjermingsverdig informasjon er gitt tilstrekkelig beskyttelse, og dermed kan være rotårsak til noen av de sikkerhetsmessige avvik og utfordringer som tilsynene har påpekt.

Tilsynet med Broadnet avdekket at det ikke var gjennomført tilstrekkelige og relevante risiko- og sårbarhetsanalyser av egne styringssystemer, samt av risikoer eller sårbarheter knyttet til tjenesteutsetting til et land som det i veiledningen fra Nkom er vist til å ha en høy risiko. Tilsynene har avdekket at virksomhetenes ledelse ikke i tilstrekkelig grad har dokumentert hvilken risiko de velger å akseptere, hvilke risikoer som må håndteres og hvilke tiltak som skal utredes og iverksettes.

3.4 Evaluering, kontroll og revisjon

Tilsynene avdekket at det ikke var gjennomført en systematisk og helhetlig evaluering av den forebyggende sikkerhetstjenesten hos virksomhetene. NSM registrerte imidlertid ved sine tilsyn at mange sikkerhetsmessige forhold var løpende adressert og håndtert.

Ved tilsynene med Nødnett ble det avdekket at det ikke var inngått sikkerhetsavtaler med alle underleverandører der det var nødvendig.

Det forelå ulik oppfatning mellom DSB og hovedleverandør for Motorola om hvem som hadde ansvaret for sikkerhetsmessig oppfølging av underleverandører, noe som medførte at slik oppfølging ikke i tilstrekkelig omfang ble gjennomført med alle relevante underleverandører.

Broadnet hadde ikke kontrollrutiner på plass som kunne oppdage om det var gitt tilganger ut over det som var tilsiktet.

3.5 Bruk av arbeidskraft uten autorisasjon/sikkerhetsklarering

Driften av Nødnett er organisert slik at det blir benyttet et høyt antall personer med relativt løs tilknytning til Norge og de skjermingsverdige objektene. Både utenlandske statsborgere bosatt i utlandet og ressurser innleid fra bemanningsselskaper, benyttes i driften. Dette kan innebære økt spredning av sensitiv og gradert informasjon om de skjermingsverdige objektene, og dermed økt risiko for etterretningsvirksomhet og sabotasje.

Det forhold at det er satt krav til sikkerhetsklarering og/eller autorisasjon for tilgang til skjermingsverdige objekter er utfordrende. Dette fordi utenlandsk arbeidskraft uten vesentlig tilknytning til Norge ble benyttet i utstrakt grad. Det ble avdekket hos tilsynsobjektene at personell fra utlandet har hatt tilgang til skjermingsverdige objekter uten gyldig sikkerhetsklarering eller autorisasjon.

Siden personellressursene som benyttes for drift av Nødnett i stor grad er basert på innleid personell og utenlandske statsborgere, kan det innebære at man i mindre grad har kontroll på ressurstilgangen. Dette utgjør en sårbarhet med hensyn til å sikre at den kompetansen som er nødvendig for drift av Nødnett er tilgjengelig.

3.6 Avgrensning av skjermingsverdige objekter

Under tilsynene, både med Nødnett og Broadnet, ble det avdekket uklar avgrensning av hva som faktisk inngikk som en del av de skjermingsverdige objektene. Videre var ikke alle avhengigheter til andre objekter eller funksjoner kartlagt og meddelt de virksomheter som rår over disse. Uklar avgrensning av skjermingsverdige objekter og manglende kartlegging av avhengigheter innebærer en risiko for at hensiktsmessige og tilstrekkelige sikringstiltak ikke blir iverksatt.

3.7 Om ansvar for korrigering av avvik

Det er DSB som anskaffende myndighet og eier av de skjermingsverdige objektene i Nødnett som må bære hovedansvaret for å korrigere avvikene som NSMs tilsyn har avdekket. Imidlertid burde Motorola som hovedleverandør til Nødnett vært den nærmeste til å opplyse DSB om både teknologiske og andre sårbarheter. For enkelte områder har Motorola hatt direkte påvirkning på valg av løsning og sikkerhetstiltak, herunder hvilket personell som benyttes for å bekle stillinger som gir tilgang til skjermingsverdige objekter i Nødnett.

Tilsynsrapportene for DSB og Motorola må sees i nær sammenheng. For å redusere sårbarheter i forbindelse med Nødnett er det helt avgjørende at Motorola bidrar aktivt i samarbeid med DSB.
NSM bemerker at Motorola har et selvstendig ansvar for å etterleve krav om tilgang til skjermingsverdige objekter.

4. Reaksjonsformer

Tilsyn med Broadnet er gjennomført med ekomloven som hjemmelsgrunnlag, mens tilsynene med DSB og Motorola er gjennomført med sikkerhetsloven som hjemmelsgrunnlag. De to regelverkene hjemler ulike reaksjonsformer. Eksempelvis gir ekomloven hjemmel til å gi overtredelsesgebyr, det gjør ikke sikkerhetsloven. Imidlertid er det foreslått tilsvarende reaksjonsformer i forslag til ny sikkerhetslov (Prop. 153 L (2016–2017)).

NSM har ved tilsynene med DSB og Motorola avdekket flere alvorlige avvik fra sikkerhetsloven med forskrifter. NSM har gitt tilsynsobjektene pålegg om å korrigere avvikene for å bringe forholdene i samsvar med regelverket. DSB skal innen 1. desember 2017 fremlegge en tidfestet handlingsplan for korrigering av avvikene ovenfor NSM. Motorola skal bidra til denne planen. Det er presisert i pålegget at utarbeidelse av handlingsplanen ikke skal være til hinder for at korrigering av avvikene startes umiddelbart for å redusere risiko. DSB er videre pålagt å jevnlig rapportere til NSM om framdriften i arbeidet med korrigering av avvikene.

Nkom har ved tilsynet med Broadnet avdekket flere alvorlige avvik fra ekomloven med forskrifter. Nkom har gitt Broadnet pålegg om å korrigere avvikene for å bringe forholdene i samsvar med regelverket. Det er gitt pålegg om umiddelbar korrigering av ett avvik, øvrige avvik skal korrigeres innen 26. januar 2018. Nkom har varslet Broadnet om at de vil bli ilagt et overtredelsesgebyr for forholdet. Nkom vil komme nærmere tilbake til utmåling av gebyret gjennom et skriftlig varsel.

DSB har ikke påklaget pålegget, for Motorola og Broadnet har klagefristen ennå ikke gått ut.

5. Regelverk

Etterlevelse av regelverkene krever at virksomhetenes ledelse avsetter tilstrekkelige ressurser og kompetanse til å sette seg inn i og implementere de gjeldende krav. I den grad virksomhetene opplever at det kan være tvil om hvordan regelverket skal forstås må de søke veiledning hos fagmyndighetene.

På bakgrunn av tilsynene som er gjennomført med hjemmel i ekomloven og sikkerhetsloven med forskrifter, kan tilsynsmyndighetene ikke se at utfordringene som er avdekket skyldes mangelfullt regelverk, men derimot manglende etterlevelse av gjeldende regelverk.

Nkom er sektormyndighet i ekomsektoren og fører tilsyn med objektsikkerhet etter forskrift om objektsikkerhet. Dette innebærer at Nkom ikke har påleggsmyndighet for de særskilte krav i objektsikkerhetsregelverket som ikke dekkes av ekomregelverket. Denne problemstillingen er viktig at adresseres når den nye sikkerhetsloven med forskrifter skal innføres.