Nasjonal kommunikasjons-myndighet

DSB - Direktoratet for samfunnssikkerhet og beredskap
Postboks 2014
3103 TØNSBERG

Vår ref.:1800753-6 -
Vår dato: 4.6.2019

Deres ref.:
Deres dato:

Saksbehandler: Janiche Solheim Justnes

Til informasjon: Brannvern - Klarering av personell

Nasjonal kommunikasjonsmyndighet (Nkom) mottok en henvendelse fra Telenor Norge AS (Telenor) angående utfordringer tilknyttet tilfredsstillende brannvern i deres skjermingsverdige objekt. Konkret gjaldt saken et brev Telenor mottok fra Telenor Eiendom den 28. januar 2018 som viste til brev Telenor Eiendom hadde mottatt fra Skien brannvesen 11. januar 2019 i forbindelse med et gjennomført tilsyn med et av Telenors fjellanlegg.

Vedlagt er Nkoms svar til Telenor på problemstillingen. Nkoms vurdering er at personell som skal gis tilgang til hele anlegget, tilegne seg god kjennskap til sikringstiltak i objektet og få tilgang til kunnskap om eventuelle svakheter ved anleggene må sikkerhetsklareres og/eller adgangsklareres. Dersom noen kun skal ha redusert tilgang til anlegget kan eventuelt andre tiltak vurderes.

Med hilsen

Svein Sundfør Scheie
seksjonssjef

Janiche Solheim Justnes
rådgiver

Dokumentet er godkjent elektronisk og ekspedert uten underskrift

Nasjonal kommunikasjonsmyndighet
Besøksadresse:
Nygård 1, Lillesand

Postadresse:
Postboks 93
4791 LILLESAND

Tel: 22 82 46 00
Fax: 22 82 46 40
firmapost@nkom.no

NO 974 446 871
www.nkom.no

Nasjonal kommunikasjons-myndighet

Telenor Norge AS
Postboks 800
1331 FORNEBU

Vår ref.:1800753-3 -
Vår dato: 22.5.2019

Deres ref.:
Deres dato:

Saksbehandler: Janiche Solheim Justnes

Brannvern - Klarering av personell

Nasjonal kommunikasjonsmyndighet (Nkom) har mottatt henvendelse fra Telenor Norge AS (Telenor) angående utfordringer tilknyttet tilfredsstillende brannvern i deres skjermingsverdige objekt. Konkret gjelder saken et brev Telenor har mottatt fra Telenor Eiendom den 28. januar 2019 som viser til et brev Telenor Eiendom har mottatt fra Skien brannvesen 11. januar 2019 i forbindelse med et gjennomført tilsyn med et av Telenors fjellanlegg hvor følgende står:

«Ut fra dagens situasjon hvor brannvesenet ikke har muligheter til å gjennomføre inspeksjonsrunder, blir konsekvensen at brannvesenet av sikkerhetsmessige hensyn ikke kan sende utrykningspersonell/røykdykkere inn i bygget ved hendelser. Eiere av anlegget må se konsekvensen av valgte løsning.»

Telenor Eiendom skriver i deres brev til Telenor at de ser med stor bekymring på denne situasjonen hvor de potensielt kan risikere alvorlige hendelser uten at liv og helse kan ivaretas på en forsvarlig måte. Som en konsekvens av denne situasjonen kan ikke Telenor Eiendom garantere tilfredsstillende brannvern og de ser på det som svært sannsynlig at de fremover kommer til å oppleve tilsvarende avvik for andre anlegg med påfølgende krav om stenging.

Bakgrunn

Telenor forvalter kritisk infrastruktur som er viktig for at det norske samfunnet skal fungere. Beskyttelse av denne infrastrukturen er viktig, og Telenor er på bakgrunn av dette underlagt sikkerhetsloven[1]. Flere av Telenors anlegg er etter gammel lov utpekt og klassifisert av Samferdselsdepartementet som

[1] *Lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (Gammel lov) (Er direkte underlagt ny sikkerhetslov (lov av 1. juni 2018 nr. 24 om nasjonal sikkerhet) inntil nytt utpekingsvedtak foreligger)*

Nasjonal kommunikasjonsmyndighet
Besøksadresse:
Nygård 1, Lillesand

Postadresse:
Postboks 93
4791 LILLESAND

Tel: 22 82 46 00
Fax: 22 82 46 40
firmapost@nkom.no

NO 974 446 871
www.nkom.no

skjermingsverdige, og frem til nye virksomheter er pekt ut vil de virksomhetene som er underlagt gjeldende lov, være underlagt ny lov.

For skjermingsverdige objekter er det et lovpålagt krav å sikre alt personell som skal tildeles adgang til skjermingsverdige objekter/arealer først må sikkerhetsklareres og/eller autoriseres. Ved ny lov kommer også begrepet adgangsklarering inn for adgang til skjermingsverdige objekter.

Hjemmelsgrunnlag

Sikkerhetslovens formål er å bidra til å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser. Videre skal sikkerhetsloven forebygge, avdekke og motvirke sikkerhetstruende virksomhet og sikkerhetstiltak skal gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

Ny sikkerhetslov legger større vekt på hva virksomhetene skal oppnå, og ikke i like stor grad hvordan de oppnår det. Virksomhetene har selv ansvaret for å regelmessig gjennomføre vurderinger av risiko og iverksette forebyggende sikkerhetstiltak for å oppnå forsvarlig sikkerhet.

Loven beskytter skjermingsverdig verdier. En skjermingsverdig verdi kan være:

- informasjon
- informasjonssystem
- infrastruktur
- objekt

Hvorvidt verdien er skjermingsverdig eller ikke, vurderes opp mot hvilken betydning verdien har for nasjonale sikkerhetsinteresser og grunnleggende nasjonale funksjoner.

Den enkelte virksomhet som er underlagt sikkerhetsloven, vil etter de nye reglene få et større selvstendig ansvar for egen forebyggende sikkerhet, som blant annet vurderingen av risiko og valget av sikkerhetstiltak.

Sikkerhetstiltak

Virksomhetsikkerhetsforskriften[2] § 60 angir at virksomhetene skal vurdere om andre sikkerhetstiltak enn adgangsklarering er tilstrekkelig for å oppnå forsvarlig sikkerhet. Dersom andre sikkerhetstiltak ikke gir forsvarlig sikkerhet kan adgangsklarering benyttes. En adgangsklarering vil være gyldig for alle typer objekter eller infrastruktur med krav om samme type adgangsklarering.

---

[2] *Forskrift av 20. desember 2018 nr. 2053 om virksomheters arbeid med forebyggende sikkerhet*

Objekter i ekomsektoren vil normalt ikke ha personell tilstede daglig og vil være avhengig av gode sikkerhetstiltak og overvåking. Objektene er sikret ut fra hvor viktig nettutstyret i objektet er. Ekomtilbyderne skal ha forsvarlig skallsikring for sine objekter for å forhindre at uvedkommende kan ta seg frem til eller påføre skade på nettutstyret.

Etter Nkoms vurdering vil det være vanskelig å oppnå forsvarlig sikkerhet uten at personell som gis selvstendig adgang til skjermingsverdige objekter i ekomsektoren adgangsklareres. Fysisk tilgang til Telenors skjermingsverdige objekter vil kunne forenkle tilsiktete angrep, noe som vil kunne gi et skadepotensiale utover det enkelte fysiske skjermingsverdige objektet.

Nkoms vurdering er at personell som skal gis tilgang til hele anlegget, tilegne seg god kjennskap til sikringstiltak i objektet og få tilgang til kunnskap om eventuelle svakheter ved anleggene må sikkerhetsklareres og/eller adgangsklareres. Dersom noen kun skal ha redusert tilgang til anlegget kan eventuelt andre tiltak vurderes.

Potensielle mål for ikke-statlig terror eller statlig sabotasje

Ved vurdering om bruk av adgangsklarering fremgår det av klareringsforskriften § 15 at dersom objektet eller infrastrukturen kan være mål for statlig sabotasje eller andre tilsiktede anslag fra annen stat kan departementet fatte vedtak til utvidet adgangsklarering.

Objektene som er utpekt i ekomsektoren inngår som en del av kritisk infrastruktur. De skjermingsverdige objektene inneholder nettutstyr som utgjør grunnstammen i nasjonal ekominfrastruktur, ved vurderingen av sikringstiltak og bruk av adgangsklarering må dette vektlegges.

Telenor har bl.a. etter egne skadevurderinger tidligere vurdert sine teletekniske skjermingsverdige objekter til å ikke være utsatt for terror. Lysne I-utvalgets rapport skrev følgende:

> *«Telenors kjerneinfrastruktur inngår som en komponent i nær sagt alle digitale verdikjeder. Et utfall i denne får derfor alvorlige og samtidige konsekvenser på de aller fleste samfunnsområder, og for alle de kritiske samfunns-funksjonene som er omtalt i denne rapporten. Viktige samfunnsfunksjoner av nasjonal betydning har en høy avhengighet til ekomtjenester.»*

Basert på Lysne I-rapporten og nye skadevurderinger har Telenor nå kommet frem til at det må forventes at spesielt Telenors skjermingsverdige objekter kan være potensielle mål for statlig sabotasje og/eller andre tilsiktede anslag fra en annen stat.

Videre peker Telenor på at det i utgangspunktet vil være vanskelig å vurdere de enkelte objekter opp mot hverandre med hensyn til om det ene eller det andre objektet er mer utsatt for tilsiktet anslag fra annen stat. Skadepotensialet og eventuelle konsekvenser må anses like alvorlig og omfattende uavhengig av hvilket objekt som blir utsatt for terror, statlig sabotasje og/eller anslag fra en annen stat. Nkom er enig i Telenors vurderinger om det store skadepotensialet og behovet for å beskytte objekter mot tilsiktede anslag.

Ordinær adgangsklarering/utvidet adgangsklarering

Det fremgår av klareringsforskriften et skille mellom «adgangsklarering» og «utvidet adgangsklarering», jf. klareringsforskriften § 17:

> *«§ 17. Vurderingsgrunnlaget for adgangsklarering*
> *En avgjørelse om adgangsklarering skal minst bygge på forholdene i sikkerhetsloven § 8-4 fjerde ledd bokastav a, b, d, l og m. I vurderingen av forhold angitt i bokstav a skal det særlig legges vekt på opplysninger om ikke-statlig terror, attentat eller annen alvorlig kriminalitet.*
>
> *En avgjørelse om utvidet adgangsklarering skal minst bygge på forholdene i sikkerhetsloven § 8-4 fjerde ledd bokstav a, b, d, l, m, k og n. I vurderingen av forhold angitt i bokstav a skal det særlig legges vekt på opplysninger om statlig sabotasje, attentat eller liknede.»*

Ordinær adgangsklarering innebærer en mindre omfattende personkontroll enn utvidet adgangsklarering. Ordinær adgangsklarering kan benyttes ved skjermingsverdige objekter og infrastruktur som kan være et mål for ikke-statlig terror, attentat eller annen alvorlig kriminalitet, mens utvidet adgangsklarering kan benyttes ved skjermingsverdige objekter eller infrastruktur som kan være et mål for statlig sabotasje eller andre tilsiktede anslag fra en annen stat.

Nkoms vurdering

Fysisk tilgang til objekter som er underlagt sikkerhetsloven gir tilgang til informasjon som alarmering, kameraovervåking, nødutganger og rømningsplaner mm. Slik kjennskap kan forenkle tilsiktet angrep, og kan medføre utfall av sentrale komponenter/tjenester som er lokalisert i objekter og vil kunne få alvorlige konsekvenser på mange samfunnsområder, herunder viktige funksjoner og tjenester innenfor Totalforsvaret.

Personellsikkerhet er en svært viktig faktor i sikringen av skjermingsverdige objekter, og for å møte trusselen om etterretning og sabotasje er Nkoms vurdering at personell som skal gis adgang til Telenors skjermingsverdige objekter som et minimum må tilfredsstille krav til adgangsklarering for utpekte objekter klassifisert VIKTIG og tilfredsstille krav til utvidet adgangsklarering for utpekte objekter

klassifisert KRITISK. Videre forutsetter Nkom at det gjennomføres autorisasjonssamtale før adgang til objekter blir innvilget.

Det er departementene som etter den nye sikkerhetsloven kan sette krav til *adgangsklarering* for adgang til skjermingsverdige objekter og infrastruktur. I de tilfeller hvor departementene ennå ikke har endret krav til sikkerhetsklarering for tidligere utpekte skjermingsverdige objekter, så gjelder kravet til sikkerhetsklarering fortsatt.

Nkom er av den oppfatning at for planlagt arbeid fra tilsynsmyndigheter, herunder branntilsyn og brannvesen, må det være mulig å sikkerhetsklarere personell som skal gjennomføre tilsynet. Nkom kan ikke se at det skal gjelde andre regler for planlagte branntilsyn, enn ved andre tilsyn som krever at personellet er sikkerhetsklarert/adgangsklarert.

Nkom vil samtidig få presisere at krav til sikkerhetsklarering/adgangsklarering til skjermingsverdige objekter ikke gjelder ved nødrett, hvor brannvesenet rykker ut ved hendelser for å redde liv eller helse. Kravet til klarering gjelder kun planlagt arbeid fra tilsynsmyndigheter, herunder branntilsyn/brannvesenet, hvor personell gis tilgang til hele anlegget, tilegner seg god kjennskap til sikringstiltak i objektet og får tilgang til kunnskap om eventuelle svakheter ved anleggene.

Med hilsen

Svein Sundfør Scheie
seksjonssjef

Janiche Solheim Justnes
rådgiver

Dokumentet er godkjent elektronisk og ekspedert uten underskrift