Forsvarsdepartementet
Pb 8126 Dep
0032 Oslo

Vår dato
01.10.2018

Vår referanse
2018-4128

Deres dato
02.07.2018

Deres referanse
2015/3139-254/FD V 3/ENWA

HØRING – FORSKRIFTER TIL NY SIKKERHETSLOV

Telenor Norge AS (heretter Telenor) viser til Forsvarsdepartementets høringsbrev av 2. juli 2018 vedrørende høring på forslag til forskrifter til ny sikkerhetslov.

Telenor anser at det er en hensiktsmessig inndeling i tre forskrifter og gir herved sine kommentarer og innspill til disse. Vi har valgt å kommentere på tvers av forskriftene på følgende 9 områder:

1. Beskyttelse av skjermingsverdige objekter og infrastrukturer
2. Generelle krav til beskyttelse av skjermingsverdige verdier
3. Klassifisering av skjermingsverdige objekter og infrastruktur
4. Beskyttelse av skjermingsverdige informasjonssystemer
5. Personellsikkerhet
6. Grunnleggende nasjonale funksjoner
7. Nasjonalt varslingssystem for digital infrastruktur (VDI)
8. Økonomiske og administrative konsekvenser
9. Ikrafttredelse og overgangsbestemmelser

Oppsummert anser vi det som positivt at det åpnes opp for å utpeke kontroll- og styringssystemer som skjermingsverdige systemer på forskjellige klassifiseringsnivåer. Det er imidlertid utfordrende å knytte de grunnleggende nasjonale funksjoner (GNF) sammen med det som er funksjoner (telekommunikasjonstjenester) og kritisk infrastruktur, regionalt og nasjonalt. Dette bør det etableres et rammeverk for ved tett samarbeid mellom myndigheter og tilbydere.

I den nye sikkerhetsloven med forskrifter er det beskrevet få definisjoner, og dette kan være hensiktsmessig da det gir mulighet for at vi som virksomhet kan utvise et visst skjønn. Telenor ser imidlertid behov for å få avklart noen begreper slik at det sikrer konsistens på tvers av samfunnskritiske aktører med hensyn på hvordan de skal forstås. Bruken av adgangsklarering/utvidet adgangsklarering, sikkerhetsklarering og klarering på vilkår må etter Telenors oppfatning tydeliggjøres/ konkretiseres ytterligere slik at det vil praktiseres helhetlig og at det er forståelig hva som kan benyttes når. Telenor anbefaler også å tydeliggjøre/definere begrepet «*befolkningens grunnleggende sikkerhet*» i tråd med lovgivers intensjon, da det er stort tolkningsrom.

Telenor har i tidligere høringsinnspill pekt på behovet for å sikre at vi har tilgang til ressurser som har ekspertkompetanse og kapasitet i en global leverandørverdikjede. I høringsnotatet fremkommer slike hensyn med tydelighet og vi håper at praksisen som skal etableres for de ulike klareringsnivåer og autorisasjon utformes i tråd med dette. Det beste er naturligvis at dette uttrykkes tydeligere i selve

forskriften. I kjølvannet av ny personopplysninglov ser Telenor positivt på at Forsvarsdepartementet presiserer og føyer til nye bestemmelser i forslaget til nye forskrifter, som er med på å tydeliggjøre forholdet til personvernregelverket. Telenor savner likevel en nærmere generell omtale fra Forsvarsdepartementet om de motstridende hensyn som gjør seg gjeldende når sikkerhetshensyn nødvendiggjør regler som går på bekostning av den enkeltes personvern.

Telenor har tidligere påpekt behovet for tverrsektoriell koordinering og oppfatter at den nye sikkerhetsloven legger til rette for det. En del av ansvaret for oppfølging av virksomhetene tillegges imidlertid de spesifikke sektorene. Dette kan medføre at vi nasjonalt sett får utilstrekkelig helhetlig risikoforståelse og vi anbefaler at NSM som ansvarlig myndighet sikres kapasitet til å kunne jobbe tett med sektormyndigheten. Det betyr at sikkerhetsmyndighetene blir en aktiv pådriver for arbeidet og gjennom det sikrer helhetlig tilnærming til blant annet utpeking, sårbarhets- og risikovurdering, bruk av standarder og gjennomføring av tilsyn.

I det videre arbeid med implementering av ny sikkerhetslov med forskrifter må det tas hensyn til den økonomiske byrdefordelingen mellom private rettssubjekter og myndigheter. Krav til sikringstiltak må stå i et rimelig forhold til kostnadene for aktørene, og det bør ikke være uklarheter knyttet til myndighetens håndtering av merkostnadene. Sikkerhetstiltak bør ikke redusere virksomhetenes konkurranseevne ved å påføre urimelige kostnader.

Videre stilles det krav om at den virksomhet som ikke selv kan redusere sin avhengighet av annet objekt eller infrastruktur, skal varsle virksomheten som råder over objektet eller infrastrukturen. Telenor mener det er vesentlig at prinsippet om at den som utløser avhengigheten må bære kostnadene forbundet med dette.

1. Beskyttelse av skjermingsverdige objekter og infrastrukturer

Skadevurdering

Det er i Virksomhetsforskriften § 52 anført vurderingskriterier som virksomheten skal legge vekt på ved utarbeiding av skadevurderinger.

Vurderingskriteriet i § 52 bokstav c omfatter «*i hvilken grad objektets eller infrastrukturens funksjon kan gjenopprettes eller erstattes*». Tidsaspektet for gjenoppretting/erstatning av funksjon er en vesentlig vurderingsfaktor. Svaret på formulering av bokstav c vil svært ofte være positivt at gjenoppretting/ erstatning av funksjon vil være mulig, men kan ta svært lang tid.

- Anbefaling: Telenor anbefaler departementet å inkludere tidsaspektet for gjenoppretting/ erstatning av funksjonen som en del av vurderingskriteriet «*i hvilken grad*». Det vil være naturlig å relatere tidsaspektet til samfunnsmessige konsekvenser.

Vurderingskriteriet i § 52 bokstav d introduseres begrepet «*befolkningens grunnleggende sikkerhet*». Begrepet blir ikke tydeliggjort (omtalt) eller definert i høringsnotatet og bør derfor defineres nærmere i forskriften. For Telenor som leverandør av kommunikasjonstjenester til hvert medlem av befolkningen, ligger det et åpenbart bredt tolkningsrom i begrepet. Et lokalt ekomutfall kan ha betydelige konsekvenser for den aktuelle befolkningen og det enkelte medlem av befolkningen sin grunnleggende sikkerhet, f.eks. manglende mulighet til å søke nødvendig hjelp gjennom ekomtjenester i en nødsituasjon, manglende mottak av viktig varsling fra myndighetene. Begrepet kan også forstås til å omhandle «*befolkningen*» i kollektiv forstand, der intensjonen bak begrepet trolig vil ha vært regionale eller nasjonale utfall som rammer sentrale samfunnsfunksjoner av avgjørende betydning for den generelle befolkningen.

- Anbefaling: Telenor anbefaler å tydeliggjøre/definere begrepet «*befolkningens grunnleggende sikkerhet*» i tråd med lovgivers intensjon, da det er stort tolkningsrom.

Forsvarlig sikkerhetsnivå for klassifiserte objekter og infrastruktur

Beskrivelsen av skadevurdering og tiltak i Kapittel 7 i Virksomhetsforskriften er noe mangelfull i forhold til sterkt distribuerte infrastrukturer. Telenors kommunikasjonsinfrastruktur består, foruten fysiske installasjoner som huser logiske funksjoner av varierende kritikalitet for vesentlig funksjon, av kabelføringer gjennom det ganske land. Bruk av sikringsstyrker (§ 54) og adgangsbegrensninger fremstår for de fleste tilfeller urealistisk for denne delen av infrastrukturen. Det samme gjelder fysisk sikring, der selv relativt godt nedgravde kabler er sårbare for fysiske anslag og ytterligere fysisk sikring fremstår både urealistisk og ineffektivt. Dette bør vurderes opp mot begrensningen i lovens § 4-3 om at «kostnadene ved sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås med tiltaket», og det må gjøres vurdering opp mot «at virksomhetene ikke skal ha flere eller mer omfattende sikkerhetstiltak enn det som er nødvendig for å oppnå et forsvarlig sikkerhetsnivå». Vi merker oss imidlertid at § 53 e-f ikke stiller krav om å avverge, men kun begrense tap av (vesentlig) funksjon. Dette er i tråd med Telenors tilnærming til funksjonskontinuitet i nettene gjennom å bygge både nasjonal og regional redundans. I § 53 g-h stilles krav til å avverge tap av funksjon / rettsstridig overtakelse (KRITISK / MEGET KRITISK).

Det er åpenbart ønskelig å avverge, og rimelig å stille krav til at det treffes tiltak innrettet mot å avverge. Etter Telenors oppfatning vil imidlertid et absolutt krav til å faktisk avverge tap av funksjon/rettsstridig overtakelse, ikke være mulig å sikre fullt ut. Kravet til Forsvarlig Sikkerhetsnivå i g-h bør derfor endres/nyanseres slik at kravet er innfridd når virksomheten har begrenset / iverksatt tiltak egnet til å avverge tap av funksjon / rettstridig overtakelse.

- Anbefaling: Telenor anbefaler at kravet om å kunne avverge funksjonstap / overtakelse i § 53 g-h i Virksomhetsforskriften endres *til slik at kravet er innfridd når virksomheten har begrenset / iverksatt tiltak egnet til å avverge tap av funksjon / rettstridig overtakelse.*

Departementet ber om høringsinstansenes syn på om det bør gis mer detaljerte krav til sikring av infrastruktur. Forskriftene er gjeldende for ulike typer infrastruktur. Selv innenfor sammenlignbare infrastrukturer består disse av forskjellig teknologibase som kan være avgjørende for valg av tiltak på detaljert nivå. I tillegg er både teknologi i infrastrukturen, tilgjengelige tiltak og kunnskap om trusselaktørenes kapabiliteter i relativt rask og vedvarende utvikling, hvilket påvirker innretningen av tiltak på detaljert nivå.

- Anbefaling: Telenor anbefaler at det ikke gis detaljerte krav til sikring av infrastruktur, men snarere fokuserer på utbyttet av appliserte tiltak i form av opprettholdelse av de(n) kritiske funksjon(er) og kontroll over denne/disse.

2. Generelle krav til beskyttelse av skjermingsverdige verdier

Plikt til å håndtere risiko

Departementet ber om høringsinstansenes syn på innretningen om hvordan risiko skal håndteres. § 12 Plikt til å håndtere risiko lyder «*Virksomheten skal håndtere risiko for å oppnå et forsvarlig sikkerhetsnivå jf. §§ 20, 32, 45 og 53.*» Dersom formuleringen «*for å oppnå*» skulle forstås som et krav til det faktiske resultatet av risikohåndteringen, ville det være en vesentlig forskjell fra en føring om innretning på risikovurdering og målsetning for forannevnte.

- Anbefaling: Telenor mener formuleringen bør tydeliggjøres for å avklare at «*for å oppnå*» skal forstås som krav til risikovurderingens og håndteringens målsetning og innretning.

Departementet omtaler i høringsnotatets kap. 7.3.2 at «*Risikoen kan håndteres helt eller delvis ved at virksomheten* […] *aksepterer den, f.eks. fordi kostnadene ved sikkerhetstiltak ikke står i et rimelig forhold til risikoreduksjonen.*» Dette gir således virksomheten anledning til å akseptere risiko, også risiko utover «*ubetydelig risiko*» jf. øvrige bestemmelser i forskriftene der dette begrepet legges til grunn for et akseptert risikonivå. Telenor tolker utsagnet til å være i kontrast med påfølgende utsagn i departementets

høringsnotat, der det blant annet fremholdes at «*Bruk av sikkerhetstiltak vil være den mest vanlige måten å håndtere risiko, og vil nesten i ethvert tilfelle være en forutsetning for å oppnå et forsvarlig sikkerhetsnivå.*» og videre at «*Det sentrale er* […] *at* [risikoen] *håndteres på en slik måte at virksomheten oppnår et forsvarlig sikkerhetsnivå.*» Sett opp mot forskriftenes øvrige krav til «*ubetydelig risiko*» og «*forsvarlig sikkerhetsnivå*», samt forannevnte avklarende utsagn i høringsnotatet og ordlyden i § 12, fremstår det ikke som virksomhetene har nevneverdig handlingsrom til risikohåndtering gjennom risikoaksept motivert ut fra tiltakenes kostnadsnivå.

- Anbefaling: Telenor mener det kan være viktig og riktig å akseptere restrisiko fremfor å investere i disproporsjonalt kostbare sikkerhetstiltak. Det er etter vårt syn viktig å tydeliggjøre dette i forskriftene hvor disse begrepene er lagt til grunn slik at handlingsrommet for å gjøre kost/nytte vurdering av mulige ytterligere sikkerhetstiltak blir tydeliggjort, selv der «*forsvarlig sikkerhet*» eller «*ubetydelig risiko*» fortsatt ikke har blitt oppnådd.

Evaluering av produkter og tjenester

Telenor merker seg at det i Virksomhetsforskriften § 15 stilles krav om at det i virksomhetens sikkerhetstiltak skal benyttes evaluerte produkter og tjenester jf. § 16, og har flere kommentarer til en slik bestemmelse:

Det fremgår ikke om kravet skal forstås som et forbud mot å benytte sikkerhetstiltak som ikke møter kravet til slik evaluering.

- Anbefaling: Telenor mener at et slikt krav ikke er hensiktsmessig, men om bestemmelsen opprettholdes må det presiseres at kravet om å benytte evaluerte produkter og tjenester ikke skal forstås som et forbud mot å også benytte sikkerhetstiltak som ikke har blitt gjort til gjenstand for slik evaluering; sekundært at kravet ikke skal forstås slik for forhold nevnt i § 15 bokstav b og c.

Som del av Telenors sikring, spesielt i vår sikkerhetsovervåkning, benyttes flere spesialiserte produkter og tjenester som er ledende på sine nisje-områder. Til dels kan disse være svært «ferske», til dels kan de være nisjeprodukter i forhold til marked og anvendelse og de kan til dels ha geografisk avgrenset utbredelse med begrenset fotfeste i Europa. Kravet om å bruke evaluerte produkter og tjenester vil være til dels sterkt hemmende i forhold til å ta i bruk moderne/ledende produkter og tjenester som en del av våre sikkerhetstiltak. Om et slikt krav hadde vært gjeldende i de senere år, ville eksempelvis Telenor Norges p.t. sterke sikkerhetsovervåkning ikke latt seg realisere i takt med det eskalerende trusselbildet.

- Anbefaling: Telenor mener derfor kravet om å benytte evaluerte produkter og tjenester er uforholdsmessig hemmende for virksomhetenes mulighet til å velge, anskaffe og implementere nødvendige produkter og tjenester for å oppnå en fullgod portefølje av sikkerhetstiltak for å møte det aktuelle trusselbildet.

I Virksomhetsforskriften § 16 Evaluering av produkter og tjenester stilles det krav om at «*evalueringen skal utføres i samsvar med ISO- og IEC-standarder for evaluering av Nasjonal sikkerhetsmyndighet eller et akkreditert laboratorium som er utpekt av Nasjonal sikkerhetsmyndighet.*». Telenor er av den oppfatning at ISO/IEC-standarder har til dels svært lang endringssyklus og fremstår på flere områder (f.eks. 27000-serien) som kun et utgangspunkt for god praksis uten nødvendigvis å ta opp i seg eller hensynta relevante forhold fra nær fortid. Dette vil i forhold til evaluering av produkter og tjenester som skal være innsatsfaktor i sikkerhetstiltak egnet til å adressere gjeldende TTP (Tactics, Techniques and Procedures), benyttet av trusselaktører motivert for handlinger som bl.a. nevnt i § 15, kunne være sterkt hemmende.

- Anbefaling: Telenors syn er at en forskriftshjemlet kobling til et spesifikt standardsett med potensielt begrenset relevans og langsom endringstakt kan virke mot bestemmelsens hensikt og bør derfor unngås.

Om vi ser bort fra ovenstående kommentarer, er den eksklusive bindingen til ISO/IEC likevel begrensende idet andre rammeverk er mer relevant for (leverandører av) en del produkter og tjenester egnet til å være

innsatsfaktor i sikkerhetstiltak, f.eks. NIST-forankrede standarder og sertifiseringer. Sistnevnte kan være mer relevant å inneha for aktuelle leverandør og deres produkter/tjenester (eksempelvis USA og andre markeder utenfor Europa). Krav om at slike produkter/tjenester likevel må evalueres i samsvar med a) ISO/IEC standarder for evaluering, og b) av NSM eller laboratorium utpekt av NSM, fremstår både hver for seg og i kombinasjon som negativt innvirkende på formålet.

- Anbefaling: Telenor mener at kravene til produkter og tjenester må være relevante, tidsmessige og mest mulig effektive tiltak for å adressere gjeldende TTP benyttet av trusselaktører motivert for handlinger.

Krav til sikkerhet i anskaffelser

I Virksomhetsforskriften § 17 Krav til sikkerhet i anskaffelser stilles det krav til at «*Avtalen skal gi virksomheten rett til å undersøke at leverandøren ivaretar sikkerheten i anskaffelsen.*» Bestemmelsen kommer til anvendelse for både skjermingsverdig informasjon, informasjonssystem, objekt og infrastruktur, herunder ikke bare «*anskaffelser til*», men også «*anskaffelser som gir tilgang til*» forannevnte (jf. § 17, 1. ledd). I denne sammenheng finner Telenor det riktig å påpeke at produkter typisk omtalt som «COTS» (Commercial Off-the-Shelf) – standardiserte og allment tilgjengelige maskin- og programvareprodukter, ofte produsert av relativt store leverandørselskaper til et svært stort antall kunder – er i utstrakt bruk på områder som faller innenfor virkeområde for bestemmelsen. For slike anskaffelser, der leverandøren har lite eller ingen forhold til produktets faktiske anvendelse innenfor § 17s virkeområde hos virksomheten, fremstår det urealistisk at leverandøren vil ha evne eller vilje til å gi virksomheten slik innsynsrett som her kreves. Dette er en allerede velkjent problemstilling. Tilsvarende vil også gjelde for bruk av programvare utviklet og vedlikeholdt på frivillig basis (ofte noe unyansert omtalt som «open source»). Slik programvare er i utstrakt bruk av virksomhetene (og i omfattende bruk som komponent eller innsatsfaktor i kommersielle produkter virksomhetene benytter). Det vil ikke være mulig å inngå slik avtale som krevet i bestemmelsen med organisasjonen, stiftelsen, «kollektivet» eller den tidvis svakt formaliserte gruppen eller enkeltperson som vedlikeholder aktuell programvare.

- Anbefaling: Telenor mener derfor § 17 og/eller omkringliggende bestemmelser i Virksomhetsforskriften kap. 2, må vurderes endret/utvidet for å hensynta det forhold at virksomhetene gjør bruk av COTS maskin- og programvarekomponenter og «open source» programvare der ovennevnte forhold gjør seg gjeldende og er til hinder for gjennomføring bestemmelsen i § 17.

3. Klassifisering av skjermingsverdige objekter og infrastruktur

I Myndighetsforskriften § 1 står det at når departementene/NSM skal klassifisere skjermingsverdige objekter og infrastruktur etter sikkerhetsloven §7-1 skal de vektlegge i hvor stor grad grunnleggende nasjonale funksjoner er avhengig av objektet eller infrastrukturen og virksomhetens skadevurdering. Departementet ber om innspill på om disse kriteriene er tilstrekkelige for å kunne beslutte klassifiseringsnivå.

- Anbefaling: Telenors syn på hvorvidt kriteriene er tilstrekkelig avhenger av innholdet i skadevurderingen. Det fremstår som nødvendig at det utarbeides en mal/veiledning for skadevurderingen i samarbeid med virksomhetene i de respektive sektorene.

4. Beskyttelse av skjermingsverdige informasjonssystemer

Forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer

Departementet utdyper i høringsnotatets kap. 7.7.2 relatert til § 45 bokstav a at begrepet «*uønsket lesing*» (jf. «*beskytte data mot uønsket lesing*») skal forstås å inkludere «*alle former for uautorisert lesing av data og informasjon*», herunder også indirekte avlesning eksemplifisert ved oppfangning og tolkning av

elektromagnetisk utstråling («*TEMPEST*»). I tillegg til klassiske «sidekanal-angrep» som f.eks. avlesning av elektromagnetisk utstråling fra IKT-utstyr, monitorer, kabler, mv., er det demonstrert en rekke former for både sidekanal-angrep på naturlige emisjoner gjennom elektromagnetisme, strømforbruk, temperatur, lys og lyd, til stimulerte emisjoner av forannevnte som konsekvens av et logisk angrep eller fysisk modifikasjon. Et uavgrenset krav om beskyttelse mot «*alle former for uautorisert lesing av data og informasjon*», eksemplifisert gjennom en form for indirekte avlesning, har derfor store konsekvenser for utforming av beskyttelsestiltak. I tillegg kommer at slik beskyttelse vil kunne måtte appliseres for all infrastruktur og utstyr brukt til lesing av data – også der dette skjer på måter i tråd med god praksis der funksjonsbegrensede, konnektivitetsbegrensede og sikkerhetsovervåkede mellomliggende noder («jump environments») brukes sammen med andre sikkerhetstiltak for å skjerme fra klassiske angrep med utgangspunkt i sluttbrukerens endepunkt. Ikke bare vil en forståelse av § 45 bokstav a i tråd med høringsnotatets kap. 7.7.2 påføre oss betydelige kostnader i økt sikring av datasentra og tilliggende føringsveier; det vil også gi helt uholdbare rammebetingelser for bruk av en rekke av våre systemer, idet alle lokaler hvorfra systemene aksesseres, og sluttbrukerutstyr de aksesseres fra, vil måtte sikres tilsvarende, og fjerntilgang fremstår ikke gjennomførbart.

- Anbefaling: Virksomhetsforskriften § 45, bør tilføyes (foreslås tatt inn som 3. og 4. ledd): *«Sikkerhetstiltakene skal være tilpasset systemets skjermingsbehov.*

  Sikkerhetstiltakene skal være tilpasset systemets intenderte funksjon og bruk. Virksomheten skal søke å innrette sikkerhetstiltakene på en måte som ikke gir en uforholdsmessig byrdefull negativ innvirkning på systemets intenderte funksjon og bruk.»

- Anbefaling: Det vil subsidiært være behov for å utarbeide operasjonaliserende veileder / tilsv. relatert til § 45 bokstav a som hensyntar de skjermingsverdige informasjonssystemenes intenderte funksjon og bruk, og der kravet til å «*beskytte data mot uønsket lesing*» ikke utelukkende avveies mot informasjonens iboende skjermingsbehov, men også behovet for tilgang til informasjonen for at den, og systemet den er del av, skal kunne fylle sin funksjon.

I Virksomhetsforskriften § 45 bokstav e kreves det at virksomheten skal «*forhindre at falske data og tjenester introduseres i informasjonssystemet*», og departementet har i høringsnotatet understreket at dette er et «*krav om at slike handlinger skal stanses før handlingen har skjedd*». Høringsnotatets drøfting fokuserer forut for dette på dataintegritet. Det er ikke helt urimelig å kreve utforming av informasjonssystem eller omkringliggende systemer og grensesnitt som sikrer at innlagte eller innleste data har strukturell integritet i samsvar med predefinerte regler og algoritmer som beskriver lovlige og/eller forventede formater og verdispenn. Begrepet «*falske data*» kan imidlertid også forstås som data som utgjør uriktig informasjon om den virkelighet de utgir seg for å beskrive. Introduksjon av data som bærer denne form for falskhet er langt mer utfordrende å stanse før handlingen har skjedd. Ikke sjelden vil tilgjengelige muligheter for betryggende validering i innleggings-/innlesingsøyeblikket være begrensede. Retrospektiv / periodisk avstemming mot andre og/eller autoritative kilder, evt. avstemming med jevnbyrdige kilder der avvik dernest eskaleres til manuell behandling, er et ikke uvanlig og for mange formål adekvat risikomitigerende tiltak.

- Anbefaling: Telenor mener det absolutte kravet i § 45 bokstav e om å «*forhindre*» at falske data introduseres i informasjonssystemet må modifiseres for at det ut fra en helhetlig risikovurdering av påregnelige konsekvenser i stedet treffes tiltak for å innen rimelig tid identifisere og korrigere falske data introdusert i systemet.

Bestemmelsen i § 45 bokstav e gir videre ikke rom for vurdering og tilpasning av tiltak i forhold til hvilken risiko (potensiell konsekvens) introduksjon av forskjellig mengde falske data i informasjonssystemet vil kunne ha.

- Anbefaling: Telenor mener § 45 bokstav e må modifiseres for å gi rom for å balansere mekanismer og tiltak for å håndtere (forsøk på å introdusere og/eller forekomst av) falske data i informasjonssystemet opp mot hvilken potensiell konsekvens varierende forekomst av falske data i informasjonssystemet påregnelig vil kunne ha. Vi foreslår å bytte ordet «forhindre» med «beskytte mot».

Ordlyden i § 45 bokstav f og resonnement/omtale fremført i departementets høringsnotat av nevnte bokstav i kap. 7.7.2 avsnitt 8 samsvarer ikke. Departementet beskriver at «*intensjonen med bokstav f* [er] *å kunne forhindre sikkerhetstruende hendelser gjennom oppdagelse og tidlig varsling*». Telenor er helt enige med departementet i at tidlig deteksjon er viktig. Forventningen om at dette generelt skal medføre at sikkerhetstruende hendelser forhindres fremstår imidlertid urealistisk. § 45 bokstav f omtaler at virksomheten skal «*registrere bruk, misbruk og forsøk på misbruk*», der registrering av misbruk åpenbart innebærer at sikkerhetstruende hendelse allerede har funnet sted.

- Anbefaling: Telenor stiller seg bak nåværende ordlyd i § 45 bokstav f, men vil advare mot en forventning, slik departementet synes å gi uttrykk for, om at dette i seg selv, eller sammenholdt med øvrige krav i § 45, vil medføre at sikkerhetstruende hendelser nødvendigvis og i alle tilfeller forhindres.

I Virksomhetsforskriften § 45 4. ledd (i høringsnotatet omtalt som tredje ledd) fremholdes at «*Sikkerhetstiltak som skal virke hurtig, eller som lett kan utløse feil når de utføres manuelt, skal automatiseres.*» Telenor stiller oss bak det vi antar er intensjonene ved dette kravet og de to driverne som motiverer kravet. Det savnes imidlertid en avveining mot operasjonell risiko og potensielle konsekvenser av automatisert iverksettelse basert på potensielt feil grunnlag. Det er vår erfaring at blant annet risiko for alvorlig negativ påvirkning på produksjon av grunnleggende elektroniske kommunikasjonstjenester, potensielt i både regional og nasjonal skala, sammenholdt med risikoøkningen som følger av at en ondsinnet handling får noe lengre virkningstid som følge av menneskelig validering av tiltak før iverksettelse. Dette leder til at minste risiko oppnås ved en delvis automatisering med menneskelig kontroll før endelig iverksettelse. Telenor savner videre, på mer generelt grunnlag enn forannevnte, en avveining mot risiko som følger av at automatisert gjennomføring av sikkerhetstiltak i seg selv introduserer sårbarhet, for eksempel i form av økt risiko for tjenestenektangrep gjennom å overstimulere den automatiserte sikkerhetsmekanismen.

- Anbefaling: Telenor mener det er helt nødvendig å endre § 45 4. ledd slik at kravet er at automatisering skal vurderes for sikkerhetstiltak som skal virke hurtig eller som lett kan utløse feil når de utføres manuelt. Det er imidlertid nødvendig at dette gjøres til gjenstand for en helhetlig risikovurdering der operasjonell risiko gjennom konsekvenser av både feilaktig utløsning av automatisert tiltak og villede handlinger som søker å misbruke automatisert tiltak til å hindre systemets intenderte funksjon eller tilgjengelighet tas i betraktning. Bibehold av manuell funksjon eller delvis automatisering med menneskelig evaluering før effektuering, vurderes som alternativer til full automatisering dersom vurdering av sistnevnte viser betydelig operasjonell risiko.

Godkjenning av skjermingsverdige informasjonssystemer

I Virksomhetsforskriften § 50, 1. ledd, bokstav b stilles det krav om at mangler i sikkerhetstiltak er «*håndtert med kompenserende tiltak*» før en midlertidig brukstillatelse kan gis. Dette omtales også med tilnærmet likelydende ordlyd i høringsnotatet der departementet fremholder krav om at «*manglende grunnlag for sikkerhetsgodkjenning er kompensert*». § 50 a og b beskriver i sum en vurdering av godkjenningsmyndigheten som ligger tett opp til vurderingen godkjenningsmyndigheten skal foreta ved normal godkjenningsprosess. Kravet om kompenserende tiltak i bokstav b foreligger også uten noen ytterligere forbehold eller nivellering, hvilket må forstås som kompenserende tiltak som fullt ut mitigerer risikoøkningen som følger av mangler i de opprinnelig tilsiktede tiltak. Ut fra dette fremstår bestemmelsen tom og nærmest selvmotsigende.

- Anbefaling: Telenor ser behovet for fleksibilitet med hensyn til å gi midlertidig brukstillatelse, jamfør de eksempler på slikt behov som er fremholdt av departementet i høringsnotatet, men kan ikke se at § 50 i sin nåværende form gir tilstrekkelig handlingsrom til å fylle disse behovene. Bestemmelsene i § 50 bør endres slik at det gis tydeligere rom for mindre uttømmende vurdering og kun delvis kompenserende tiltak, basert på en risikovurdering av sistnevnte som også hensyntar systemets bruksomfang, skadepotensiale og eksponering sammen med den midlertidige brukstillatelsens intenderte varighet**.**

5. Personellsikkerhet

Høringsnotatet og forskriften henviser til adgangsklarering/utvidet adgangsklarering, sikkerhetsklarering og klarering på vilkår (stillingsklarering). Telenor er av den oppfatning at bruken av adgangsklarering/utvidet adgangsklarering, sikkerhetsklarering og klarering på vilkår må tydeliggjøres/konkretiseres ytterligere slik at det vil praktiseres helhetlig og at det er forståelig hva som kan benyttes når.

- Anbefaling: Telenor mener det må tydeliggjøres i forskriften hvordan autorisasjon for BEGRENSET kan benyttes opp imot skjermingsverdige verdier og hvilken informasjon som skal innhentes før/til autorisasjonen og evt. hvilke punkter i skjema som skal fylles ut. Informasjonen som søkes innhentet må knyttes opp til en lovhjemmel som skal oppgis for å søke om autorisasjon for BEGRENSET.

Klarering av utenlandske statsborgere

Det er positivt at det i større grad enn i dag vil være mulig å klarere utenlandske statsborgere, også de uten tilknytning til Norge, ved at det foreslås en oppmykning ved at handlingsrommet i ny sikkerhetslov §8-7 benyttes i større grad.

- Anbefaling: Telenor ønsker likevel å presisere viktigheten av å sikre en praksis om reflekterer dette, slik at man ikke blir for restriktiv og mister verdifull kompetanse grunnet for streng tolkning av loven. Telekom er en internasjonal bransje der leverandører, samarbeidspartnere, spesialkompetanse og tekniske løsninger går på tvers av landegrenser. Som det påpekes er det i noen tilfeller behov for å klarere utenlandske statsborgere som har kompetanse som ikke er tilgjengelig i Norge og som virksomheten er avhengig av. Det må derfor legges større vekt på hjemlandets sikkerhetsmessige betydning, og ikke som det praktiseres i dag hvor graden av tilknytning til Norge er en avgjørende faktor, slik at det lar seg gjøre å f.eks. benytte skandinaviske ressurser bosatt i sitt hjemland til oppgaver som krever sikkerhetsklarering og/eller autorisering for å kunne benytte eksempelvis arbeidskraft på tvers av landene.

Departementet ber om innspill knyttet til klarering/autorisasjon for utenlandske statsborgere:

- Telenor anser at det ikke er et ytterligere behov for konkretisering av vurderingstemaene (jf. ny sikkerhetslov §8-7), men det er viktig at man får en enhetlig praksis for behandling av klarering/autorisasjonssaker.
- Når det gjelder bestemmelsen i kapittel 4 i Klareringsforskriften vedrørende samtykke til å autorisere utenlandske statsborgere for BEGRENSET, så anser Telenor at det mest hensiktsmessige alternativet er at virksomhetene blir gjort kjent med NSMs vurdering av andre stater og selv vurderer den risiko autorisering av utenlandsk personell for BEGRENSET innebærer.

Personkontroll/egenopplysninger

Telenor synes at det er bra at det i Klareringsforskriften klart fremgår i §§ 7 og 9 hvilke egenopplysninger som skal gis i forbindelse med hhv. sikkerhetsklarering og adgangsklarering, samt § 27, som omhandler hvilke egenopplysninger som Sikkerhetsmyndighetene kan kreve av utenlandske statsborgere for avgjørelse om tillatelse for autorisasjon for BEGRENSET.

- Anbefaling: Telenor savner like tydelig hjemmelshenvisning i Virksomhetsforskriften for hvilke personopplysninger som kan samles inn og behandles i de tilfeller en person ikke skal sikkerhetsklareres, men må autoriseres av virksomheten for nivå BEGRENSET.

Telenor anser at det er viktig å få egenopplysninger fra den som skal klareres for å kunne kontrollere påliteligheten, samt at dette også vil øke bevisstheten til den som skal klareres/autoriseres. I Telenor har det blitt stilt spørsmål ved hvilke personopplysninger som kan kreves avgitt fra en som skal autoriseres for BEGRENSET. Dette i forbindelse med krav om utfylling av Personopplysningsblanketten (POB) som det har vært praksis for å benytte også for autorisasjon til Begrenset. Dette er en praksis som er avklart med Samferdselsdepartementet, som vår tidligere klareringsmyndighet for utenlandske statsborgere, og som har vært den som har risikovurdert om en person er autoriserbar på grunnlag av POB.

Telenor tok opp spørsmålet våren 2018 med Datatilsynet og Nkom, som igjen har vært i kontakt med NSM. Telenor oppfattet i samtale med Datatilsynet at også de har sett utfordringer med hvordan dagens forskrift om personellsikkerhet § 5-2 er formulert, samt dagens praksis med utfylling av POB, sett opp mot de krav som stilles i nylig vedtatte personopplysningslov om blant annet samtykke. Slik Telenor har oppfattet sikkerhetsmyndighetene, mener de at det på sin side er nødvendig å innhente en rekke personopplysninger også for autorisasjon for nivå BEGRENSET, og at hjemmel for dette følger av dagens Personellforskrift § 5-2, herunder også opplysninger som etter personvernregelverket omhandler særskilte kategorier av personopplysninger, slik som f.eks. helse, herunder forhold til rusmidler og straffbare forhold.

Telenor savner imidlertid en klar lovhjemmel som regulerer hvilke opplysninger som kan kreves. Slik Personellforskriften § 5-2 i dag er formulert fremstår den som uklar på dette punktet. Som følge av kravene i det nye personvernregelverk er det viktig at særlovgivningen nettopp gir en klar hjemmel som ikke sår tvil om hvordan reglene skal forstås. Det er av avgjørende betydning at særlover og forskrifter som f.eks. sikkerhetsloven og tilhørende forskrifter ikke levner tvil om hvilken adgang og lovlig behandlingsgrunnlag som foreligger hva gjelder behandling av personopplysninger i sikkerhetsøyemed.

Samtykke

Telenor registrerer at samtykke er nevnt flere steder i høringsforslaget som grunnlag for innhenting av personopplysninger. I arbeidsforhold vil ikke kravet til frivillighet være oppfylt ved bruk av samtykke grunnet den skjevhet som foreligger i styrkeforholdet mellom en arbeidsgiver og en ansatt, og den lojalitetsplikt som den ansatte må vise ovenfor arbeidsgiver. For de tilfeller en virksomhet skal autorisere for BEGRENSET eller det er snakk om sikkerhetsklarering som myndighetene vurderer, jf. klareringsforskriften § 7 og 8, må behandlingsgrunnlaget for innhenting av de nødvendige personopplysninger om de ansatte derfor være hjemlet som en plikt i forskriftene, ikke som et krav om samtykke. Telenor viser her bl.a. til fortalen til GDPR punkt 42 og 43:

> *Punkt 42:* Samtykket skal ikke anses som frivillig dersom den registrerte ikke har en reell valgfrihet, eller ikke er i stand til å nekte å gi eller trekke tilbake et samtykke uten at det er til skade for vedkommende.
>
> *Punkt 43*: For å sikre at et samtykke gis frivillig bør det ikke utgjøre et gyldig rettslig grunnlag for behandling av personopplysninger i et bestemt tilfelle dersom det er en klar skjevhet mellom den registrerte og den behandlingsansvarlige, særlig dersom den behandlingsansvarlige er en offentlig myndighet og det derfor er usannsynlig at samtykket er gitt frivillig med hensyn til alle omstendigheter som kjennetegner den bestemte situasjonen.

- Anbefaling: Dersom sikkerhetsmyndighetene mener at det er nødvending å innhente personopplysninger som opplyst i personopplysningsblanketten også for autorisasjon for nivå BEGRENSET, må dette fremgå av en klar lovhjemmel. Dersom det ikke er sikkerhetsmyndighetens hensikt, må det hjemles hvilke opplysninger sikkerhetsmyndigheten mener det er nødvendig å

innhente. Samtykke kan ikke anses for å være gyldig behandlingsgrunnlag i dette tilfelle, da det er tvilsomt om det for dette tilfelle vil være ansett for å være frivillig avgitt.

Adgangsklarering

Telenor er positive til introduksjonen av adgangsklarering som personkontrollinstrument. Vi ser imidlertid grunn til å utvide hjemmelsgrunnlaget for utvidet adgangsklarering.

Departementet har i høringsnotatets kap. 4.4 anført at «*Departementet legger til grunn at nærstående har mindre betydning for adgang til skjermingsverdig objekt eller infrastruktur, enn for tilgang til gradert informasjon.*» Departementet synes imidlertid i dette resonnementet å se bort fra at adgang til skjermingsverdig objekt eller infrastruktur i mange tilfeller gir tilsvarende anledning til å observere de forhold som er dokumentert i skjermingsverdig informasjon, eller erverve slik informasjon behandlet i/av aktuelle skjermingsverdige objekt/infrastruktur. Telenor mener det derfor er mangelfullt grunnlag for å resonnere og differensiere slik departementet her gjør, og at tilgang til skjermingsverdig objekt/infrastruktur i mange tilfeller vil medføre at skjermingsverdig informasjon «*kan gjøres tilgjengelig for nærstående dersom den som er klarert ikke overholder taushetsplikten*» tilnærmet like lett som ved direkte tilgang til skjermingsverdig informasjon, til tross for at muligheten til å gjøre dette i form av medbringelse av fysiske dokumenter kan være noe mindre.

Departementet viser i høringsnotatets kap. 4.4 videre til at «*Terskelen for at en nærstående skal kunne skade et objekt eller en infrastruktur er derimot høyere, fordi den nærstående da først må skaffe seg adgang til objektet eller infrastrukturen.*» Det er også her vanskelig å se grunnlaget for resonnementet. Adgang er på ingen måte en universell forutsetning for å kunne utnytte skjermingsverdig informasjon om et objekt eller infrastruktur til å gjennomføre skade (som heller ikke kan forstås som begrenset til destruktive handlinger, jf. drøfting om konfidensialitet, integritet og tilgjengelighet over, spesielt gjeldende for objekt og infrastrukturer som i seg selv er informasjons-/kommunikasjonsbærende). Videre vil den informasjon som nærmest av nødvendighet erverves ved adgang typisk inkludere kunnskap om hvordan adgang kan oppnås (i spennet fra metoder / prosesser / grunnlag som kan utnyttes i social engineering / grunnlagsforfalskning, via kunnskap om rutiner, sårbarheter med videre, til direkte kjennskap til adgangskoder og passord). Det er helt sikkert scenarier der departementets herværende resonnement har en viss gyldighet og terskelen er noe høyere, men vi kan ikke se at resonnementet har generell gyldighet for alle adgangsscenarier / objekter / infrastrukturer, og heller ikke at terskelen er vesentlig høyere i forhold til den angjeldende differensieringen.

I Klareringsforskriften § 15 gjenspeiles departementets vurderinger jf. de to her ovenstående avsnitt (ang. høringsnotatets avsnitt 4.4), idet vurdering av adgangsklarering kun skal legge til grunn forhold av direkte betydning for fysiske anslag (jf. sikkerhetsloven § 8-4 fjerde ledd bokstav a, b, c, l og m), mens det først ved utvidet adgangsklarering hensyntas forhold mer relatert til informasjonssikkerhet og indirekte press typisk utøvd og relatert til informasjonsinnhenting (jf. sikkerhetsloven § 8-4 fjerde ledd bokstav k og n).

- Anbefaling: Telenor mener det må tydeliggjøres, formodentlig i Virksomhetsforskriften kap. 7, at der adgangsklarering skal benyttes som virkemiddel ved adgang til skjermingsverdig system, objekt eller infrastruktur jf. § 55, skal det vurderes om adgangen innebærer implisitt tilgang eller vesentlig forenklet tilgang til skjermingsverdig informasjon, og i så fall alltid benyttes utvidet adgangsklarering.

6. Grunnleggende nasjonale funksjoner

Virksomhetsforskriften § 52 stiller krav til at «*Virksomheten skal vurdere hvilke skadefølger det kan få for grunnleggende nasjonale funksjoner om det skjermingsverdige objektet eller infrastrukturen den råder over blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse.*» Det fremkommer imidlertid ikke noen avgrensning av at dette ansvaret kun omfatter de grunnleggende nasjonale funksjoner virksomheten er

ansvarlig for, og de derav utpekte skjermingsverdige objekter eller infrastrukturer, og heller ikke at et ansvar for slik skadevurdering utover dette avhenger av at virksomheten som er ansvarlig for andre grunnleggende nasjonale funksjoner har varslet om slik avhengighet jf. 3. ledd.

Telenor mener det vil være urimelig å forvente at vi, som underlagt virksomhet, skal foreta skadevurdering i forhold til grunnleggende nasjonal funksjon som tilligger annen virksomhets ansvar, uten at denne har gitt varsling som anført i 3. ledd.

Anbefaling: 1. ledd bør derfor endres slik:
«*Virksomheten skal vurdere hvilke skadefølger det kan få for grunnleggende nasjonale funksjoner om det skjermingsverdige objektet eller infrastrukturen den råder over blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse. Virksomheten skal i skadevurderingen ikke innta andre virksomheters avhengighet til virksomhetens objekter eller infrastruktur, utover avhengigheter som er varslet iht. 3. ledd.*»

Telenor har for øvrig, på initiativ fra SD og i fellesskap med Broadnet, Telia, Nextgentel, Altibox og Ice, utarbeidet en innstilling til rammer for identifikasjon av *grunnleggende nasjonale funksjoner* (GNF) i ekom-sektoren. Vi drøfter her grensegang mot eventuelle spesifikke avhengigheter til ekom-leveranser hos virksomheter som utgjør eller har ansvar for GNF til støtte for nasjonale sikkerhetsinteresser angitt i Lov om nasjonal sikkerhet § 1-5, punktene a til d; kontra ekomtjenester som GNF til støtte for punkt e. Vi drøfter videre avgrensning mot grunnleggende ekomtjenester, faktorer som spiller inn i forhold til når det foreligger et «*helt eller delvis bortfall*» (funksjonstap, geografisk utbredelse, varighet og bortfall på tvers av aksessteknologier) og internasjonal kommunikasjon.

7. Nasjonalt varslingssystem for digital infrastruktur (VDI)

I § 12 i Myndighetsforskriften beskrives «*en nasjonal responsfunksjon for alvorlige digitale angrep*».
Det er avgjørende at virksomhetene selv har evne til å håndtere og respondere på avdekte hendelser. NSM NorCERTs kapasitet, domenekompetanse og virkemidler omhandler først og fremst å bistå virksomheter i deres egen hendelseshåndtering. Dette er da hva vi forstår som «respons» til en sikkerhetshendelse. Det fremstår derfor ikke realistisk at en responsfunksjon, slik vi forstår ordet, skal kunne etableres og vedlikeholdes som en sentralisert nasjonal funksjon.

- Anbefaling: Telenor anser begrepet responsfunksjon som unøyaktig og anbefaler at forskriften endres til å gjenspeile NSM NorCERTs primære funksjon og ansvar knyttet til informasjonsbehandling i forbindelse med deteksjon av sårbarheter og angrep, samt i bistand ved virksomhetens håndtering av hendelser. Dette betyr at NSM NorCert skal sikre, uten unødig opphold, informasjonsdeling med virksomhetene – egnet til å styrke virksomhetenes evne til å både forhindre, avdekke og håndtere angrep på/i eget domene, systemer og infrastruktur. I tillegg skal NSM NorCERT legge til rette for og understøtte, uten unødig opphold eller endring i innhold, informasjonsdeling og samhandling mellom virksomhetene (CERT- og/eller VDI-medlemmer) ved hendelser. Tilbakeholdelse av informasjon skal kun skje dersom det i enkelttilfeller er spesifikke og tungtveiende grunner for det.

§ 13 legger etter Telenors oppfatning ikke opp til den grad av informasjonsdeling som er nødvendig for å understøtte virksomhetene og deres evne til å forhindre, avdekke og håndtere angrep på/i eget domene, systemer og infrastruktur.

§ 13, 2. ledd avgrenser deling med virksomhetene til tilfeller der de er positivt identifisert som «*berørte aktører*» «*ved fare for alvorlige hendelser*». En slik restriktiv og minimal informasjonsdeling med virksomhetene understøtter verken lovens formål eller virksomhetenes evne til å ivareta sitt ansvar, men reduserer snarere verdien av den informasjon NSM besitter. Vi ser ingen grunn til at ikke

sikkerhetsfunksjonen hos virksomheter underlagt sikkerhetsloven skal kunne motta all den informasjon NSM besitter om trusler, sårbarheter og tiltak, som med noen grad av rimelighet potensielt kan bidra til virksomhetenes utøvelse av sitt ansvar og deres evne til å forhindre, avdekke og håndtere angrep.

- Anbefaling: Telenor anbefaler at § 13 bør endres slik at ordlyden i tillegg reflekterer at NSM pålegges å dele slik informasjon med virksomheter underlagt sikkerhetsloven, så langt virksomheten er sikkerhetsmessig skikket til å håndtere informasjon på aktuelle graderingsnivå, og med mindre det er spesifikke og tungtveiende grunner til å tilbakeholde informasjonen. Et forslag til ordlyd kan være; Nasjonal Sikkerhetsmyndighet skal for øvrig sikre at virksomheter underlagt sikkerhetsloven mottar den informasjon NSM besitter om trusler, angrep, sårbarheter og tiltak, som med rimelighet kan forventes å bidra til virksomhetenes utøvelse av sitt ansvar og deres evne til å forhindre, avdekke og håndtere angrep.

§ 57 gir ikke virksomhetene noen rett til innsyn i hvordan innsamlede data blir brukt, herunder hvordan disse analyseres, for hvilke formål de analyseres, i hvilken utstrekning innsamlede data eller informasjon utledet fra innsamlede data videreformidles til andre organer for støttende eller andre formål, eller hvor lenge innsamlede data lagres. § 57 gir derfor etter vår mening ikke tilstrekkelig innsyn i behandling og bruk av innsamlede data, hvilket er essensielt for at innsynsretten skal tjene sitt formål.

- Anbefaling: Avgivende virksomhets innsynsrett bør etter vår mening utvides gjennom en endring av § 57, slik at virksomheten får rett til innsyn i hvordan innsamlede data blir brukt, analysert, videreformidlet til andre parter og/eller anvendt for andre formål, samt hvor lenge innsamlede data lagres.

§ 56 omfatter ikke, jf. vår kommentar til § 57 over, tilstrekkelige krav til regulering av rammer for bruk, behandling, utveksling, foredling og oppbevaring av innsamlede data, idet den begrenser seg til å stille krav om at avtalen skal regulere behandling av data som allerede er underlagt lovbestemte krav til behandling og taushetsplikt. Dette anser vi ikke som tilstrekkelig og anser at departementet bør legge til grunn lignende rettsforståelse til grunn for virksomhetens data innsamlet av NSMs overvåkningsnoder som eksempelvis legges til grunn i norsk og europeisk personvernlovgivning, der bibeholdt eierskap til innsamlede data er et grunnprinsipp.

- Anbefaling: § 56 anbefales endret og utvidet med tydeliggjøring av at innsamlede data forblir virksomhetens eiendom. Videre må § 56 omfatte eksplisitte avgrensninger for de forannevnte forhold, der det tydelig fremgår at innsamlede data kun skal inngå i NSMs analyse, identifikasjon og bistand i håndtering av hendelser hos virksomheten som med rimelig sannsynlighet truer skjermingsverdig eller gradert informasjon, system, objekt eller infrastruktur. Sekundært til forannevnte må § 56 stille krav om at avtalen skal regulere forhold som naturlig følger av dette, herunder rammer for bruk, behandling, utveksling, foredling og oppbevaring av innsamlede data.

Departementet varsler i høringsnotatets avsnitt 7.9.2 om at «*Departementet ser imidlertid nærmere på muligheten for NSM til å kunne pålegge tilknytning til VDI*» og ber om **høringsinstansenes syn** på en slik påleggskompetanse.

Telenor oppfatter at et pålegg om å innplassere overvåkningsnoder i virksomhetenes nett og infrastrukturer kan virke mot sin hensikt. Det må derfor nøye vurderes hvordan et pålegg utformes. Den antydede uavgrensede hjemmel for NSM til å pålegge innplassering av overvåkningsnoder i virksomhetenes nett og infrastrukturer, fremstår disproporsjonal, frikoblet fra virksomhetens eget ansvar og kapabiliteter og uavstemt i forhold til rettssikkerhet, personvern og formålsavgrensning. Virksomhetens kunnskap om og evne til å håndtere (hendelser i) egne systemer og infrastruktur er helt avgjørende for å håndtere observerte hendelser hos virksomheten.

Beskrivelsen av virksomhetens samspill med NSM fremstår som til dels motstridende i forhold til ansvar for håndtering. 3. avsnitt innledes med: *«Hensikten med utplasseringen er å oppdage alvorlige digitale angrep,*

slik at disse kan håndteres, som utgangspunkt av virksomheten selv eller med bistand fra et responsmiljø.» mens det senere i samme avsnitt fremholdes: *«Dette innebærer at det må avtales nærmere i hvilke tilfeller NSM vil håndtere hendelsen, og hvordan virksomheten eventuelt skal bistå i håndteringen.»* Sistnevnte gir inntrykk av at virksomheten i liten grad er aktiv i håndteringen noe vi mener ikke er formålstjenlig eller realistisk for å sikre en god håndtering av observerte hendelser. Det er virksomheten som må være ansvarlig for håndteringen og evne å ta imot bistand fra NSM eller annen relevante parter.

- Anbefaling: En eventuell hjemmel til pålegg om innplassering av NSMs overvåkningsoder må avgrenses til å ikke omfatte innplassering i systemer og infrastruktur som understøtter eller inngår i produksjon av elektroniske kommunikasjonstjenester som tilbys den generelle befolkningen, eller inneholder informasjon om bruk av slike tjenester. Det må i tillegg tydeliggjøres at det er virksomheten som må være ansvarlig for håndtering av hendelser og ha nødvendig evne å ta imot bistand fra NSM NorCert eller annen relevante part.

Virksomheten har et selvstendig ansvar for å ivareta forsvarlig sikkerhet, et begrep som nødvendiggjør omfattende sikkerhetsovervåkning. Der virksomheten innfrir eller har pågående aktiviteter som innen rimelig tid vil føre til innfrielse av krav om forsvarlig sikkerhet, herunder også adekvat sikkerhetsovervåkning, fremstår det ikke formålstjenlig at NSM i tillegg skal kunne pålegge innplassering av sine overvåkningsnoder. Der virksomheten selv, på selvstendig basis eller også støttet av kvalifisert tredjepart, i rimelig grad ivaretar sikkerhetsovervåkning som del av sine tiltak for nødvendig sikkerhet jf. krav i lov og forskrift, bør NSM ikke ha hjemmel til å kreve innplassering av sine overvåkningsoder, men snarere pålegges å tilgjengeliggjøre relevante indikatorer og trusselinformasjon til virksomheten, for bruk i virksomhetens egne sikkerhets-overvåkningsmekanismer. Det følger av dette at begge parter må integrere sin sikkerhetsovervåkning slik at man begge veier klarer å utveksle tekniske indikatorer, rapporter og innsikt om pågående operasjoner hvor Norge kan være eller bli et mål.

- Anbefaling: Dersom en hjemmel for pålegg om innplassering av NSMs overvåkningsnoder i virksomheten likevel blir gitt, med eller uten de avgrensninger Telenor har foreslått over, anser vi at hjemmelen uansett må avgrenses i forhold til omfanget av slik innplassering. Vi finner det rimelig, proporsjonalt og tilstrekkelig at en eventuell hjemmel for pålegg om innplassering av NSMs overvåkningsnoder hos virksomheten, i tillegg til forannevnte avgrensninger, begrenses til innplassering på grensesnitt mellom virksomhetens infrastruktur og offentlig nett (Internett).

8. Økonomiske og administrative konsekvenser

I videre arbeid med implementering av den nye sikkerhetsloven, med tilhørende forskrifter, må fordeling av de økonomiske forpliktelsene mellom private rettssubjekter og myndighetene tas hensyn til. Samfunnets og nasjonens avhengighet til IKT-infrastruktur og konsekvensene ved bortfall for GNF vil kunne medføre krav til sikringstiltak hvor det må enes om en byrdefordeling mellom spesielt private rettssubjekter og myndighetene. De ulike kravene som settes må stå i et rimelig forhold til kostnadene for aktørene og mulig være en øvre grense for hvor store kostnader private virksomheter skal belastes. Det bør ikke være uklarheter knyttet til myndighetens håndtering av merkostnadene.

Telenor forventer at det vil bli stilt økte krav til sikring- og redundans til oss, ettersom vi leverer en funksjon som er viktig på tvers av alle sektorer og understøtter GNF. Det bør derfor tydeliggjøres prinsipper for hvordan merkostnader skal dekkes. Et grunnleggende prinsipp kan være er at det er den som utløser avhengigheten som også dekker den økonomiske forpliktelsen, dernest at myndighetene tar en del av den økonomiske forpliktelsen dersom merkostnadene er betydelige.

Det stilles krav til at den virksomhet som er avhengig av et objekt eller infrastruktur (og ikke kan redusere sin avhengighet) skal «*varsle den som råder over objektet eller infrastrukturen om avhengigheten*» (jf. § 52 3. ledd). Det er i høringsnotatet videre omtalt:

«*Hensikten er at virksomheten som mottar varselet da kan benytte informasjonen i sin egen skadevurdering. Bestemmelsen er imidlertid ikke ment å regulere hvilke av de to virksomhetene som plikter å iverksette tiltak i en slik situasjon. Normalt vil dette være virksomheten som er avhengig av dem andre, men dette vil kunne variere ut i fra krav i sektorlovgivningen, konsesjonsvedtak, leveranseavtalen mellom virksomhetene og andre relevante rettskilder.*»

- Anbefaling: Det er et viktig prinsipp at den som utløser avhengigheten må bære kostnadene forbundet med dette. I forslag til nye forskrifter er det ikke regulert hvem som skal dekke de eventuelle kostnadene ved varslede avhengigheter til andre objekter eller infrastruktur etter at det er utført skadevurdering og restrisikoen er vurdert. Stort sett alle virksomheter/sektorer har en eller annen avhengighet til ekom. Av den grunn vil det være nærmest umulig å utføre og vedlikeholde skadevurderingene til det enkelte objekt/infrastruktur. Telenor mener at det er vesentlig at prinsippet om at den som utløser avhengigheten må bære kostnaden tas inn i forskriftens ordlyd. Det anbefales i tillegg å tydeliggjøre myndighetenes ansvar for håndtering av merkostnader.

9. Ikrafttredelse og overgangsbestemmelser

Det er viktig at konkret frist for å tilpasse seg kravene i ny lov med tilhørende forskrifter blir satt i samråd og dialog med virksomheten selv. Hvilke kriterier som vil vektlegges i vurderingen av hva som vil være en «rimelig frist», bør fastlegges nærmere. Telenor støtter dermed departementet i at det vil være hensiktsmessig med en egen bestemmelse som regulerer hvilke momenter som skal vurderes i fastleggelsen av en konkret frist for virksomhetens sikring av et forsvarlig sikringsnivå for hvert enkelt informasjonssystem, infrastruktur, eller objekt.

- Anbefaling: I vurderingen av hva som vil være en «rimelig frist» bør følgende momenter etter vårt syn inngå:
  - Tiltakets omfang og kompleksitet for å oppfylle kravene i regelverket
  - Undersøkelser av hvor stor belastning tiltaket er for pliktsubjektet både med hensyn til økonomisk byrde og i forhold til å beslaglegge kapasitet hos interne og eksterne ressurser
  - Hvorvidt tiltaket innebærer leveranse eller tiltak fra eksterne leverandører, eller ekstern tilbyder, til den virksomheten som er pliktsubjektet
  - Hva vil anses å være utgangspunktet for en normallengde på fristen for ulike typer av tiltak, og hvilke momenter forvaltningen kan ta hensyn til i vurderingene av om det er behov for å avvike fra normalordningen.

Det er viktig at fristens lengde settes i samråd med pliktsubjektet. Det bør også fremkomme tydelig at det er departementet som har ansvaret for å ta initiativ til, og som har ansvaret for å kartlegge sentrale forhold sammen med tilbyderne for å kunne vurdere fristens lengde.

Telenor stiller seg til rådighet for ytterligere utdypning av høringssvaret.

Med hilsen
Telenor Norge AS

Hanne Tangen Nilsen
Sikkerhetsdirektør