Nasjonal sikkerhetsmyndighet

Vår saksbehandler
Plan og administrasjonsstab

Vår dato
2016-03-10

Vår referanse
A03 - S:15/04683-~~8~~ 7

Deres dato
2015-12-09

Deres referanse
15/8216

Antall vedlegg

Til
Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 Oslo
Norge

Digital sårbarhet - Sikkert samfunn - Høringssvar fra Nasjonal sikkerhetsmyndighet

1 Innledning

Nasjonal sikkerhetsmyndighet (NSM) viser til Justis- og beredskapsdepartementets (JD) brev av 09.12.15 hvor rapporten «Digital sårbarhet – sikkert samfunn» (NOU 2015:13) sendes på høring.

NSM er i det alt vesentlige enig med Digitalt sårbarhetsutvalgs[1] vurderinger og forslag til tiltak. NSM merker seg at utvalgets anbefalinger ved flere anledninger sammenfaller med NSMs anbefalte tiltak i NSMs "Sikkerhetsfaglig råd" av september 2015.[2]

NSM ønsker å knytte følgende merknader til rapporten. NSM vil bemerke at enkelte temaer med fordel kunne vært utdypet i vår høringsuttalese, men at uttalelsen da ville blitt sikkerhetsgradert. NSM kan eventuelt supplere uttalelsen i videre dialog med departementet.

2 Merknader

2.1 IKT-tilsyn

2.1.1 Behovet for styrket tilsynskompetanse

Utvalget foreslår å styrke kapasiteten ved flere sektortilsyn innen IKT-sikkerhet.[3]

---

[1] Heretter omtalt som utvalget
[2] NSM Sikkerhetsfaglig råd – overlevert til Forsvarsdepartementet og Justis- og beredskapsdepartementet 10. september 2015, heretter omtalt som SFR.

Postadresse
Postboks 814
1306 SANDVIKA

Sivil telefon/telefaks
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09
Internetadresse (URL)
www.nsm.stat.no

NSM er enig med utvalget i at tilsyn med IKT-sikkerhet i norske virksomheter bør økes. Tilsyn i regi av NSM har gjennomgående avdekket avvik og sårbarheter som virksomhetene selv burde ha oppdaget og korrigert gjennom interne sikkerhetsrevisjoner og evalueringer. NSMs erfaringer fra tilsyn med etterlevelse av lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), inntrengningstesting og erfaringer fra håndtering av IKT-hendelser også utenfor sikkerhetloven viser at sårbarhetene i norske virksomheter er store, og at forebyggende tiltak ikke i nødvendig grad er implementert i virksomhetene. Arbeidet med forebyggende sikkerhet mangler ofte lederfokus. Dette gjelder for statlig virksomhet på ulike nivåer, og i private og offentlige virksomheter. Konsekvensen er at risikostyringen ofte er utilstrekkelig.

2.1.2 Hvordan oppnå styrket kompetanse og kapasitet

NSM har i dag høy kompetanse på IKT-sikkerhetsområdet, men begrenset kapasitet til å gjennomføre tekniske IKT-sikkerhetstilsyn. Det finnes i dag over 40 statlige tilsyn. De fleste av disse kontrollerer innenfor sine respektive regelverk at virksomhetene har et styringssystem eller internkontrollsystem på plass. Kompetansen til å gjennomføre tekniske IKT-sikkerhetstilsyn er ikke god nok hos mange tilsynsmyndigheter. NSM anser at det ikke er tilstrekkelig IKT-sikkerhetskompetanse nasjonalt til at alle tilsynsmyndigheter kan bygge opp egne IKT-sikkerhetsmiljøer.

NSM mener det bør utvikles felles grunnleggende retningslinjer og metoder for utførelse av teknisk IKT-sikkerhetstilsyn. NSM er det nasjonale fagmiljøet for IKT-sikkerhet, og det er en naturlig del av NSMs rolle å inneha en tung og bred kompetanse innen IKT-sikkerhetsområdet.

NSM mener derfor av samfunnsøkonomiske hensyn, og for ikke å bygge dublerende kompetansemiljøer, at tilsynskompetansen innen teknisk IKT-sikkerhet bør samordnes ved at NSM tilføres ressurser for å etablere en kapasitet som kan gi tilsynsstøtte til andre sektortilsyn på IKT-sikkerhetsområdet. Dette innebærer at NSMs revisjonspersonell bistår det enkelte sektortilsyn med teknisk IKT-sikkerhetskompetanse til å gjennomføre tilsyn etter sektormyndighetenes eget regelverk. Dette har NSM også foreslått i SFR.[4]

Utvalgets tilnærming er at sektorene og tilsynsvirksomhetene på lengre sikt må etablere egen IKT-sikkerhetskompetanse. NSM ser viktigheten av at sektorene etablerer robuste IKT-miljøer, men vil samtidig, i liket med utvalget, poengetere at det da er meget viktig at det etableres fellesarenaer for erfaringsutveksling og dialog mellom sektortilsyn og tverrsektorielle tilsyn.

2.2 Avdekke og håndtere digitale angrep

Utvalget vurderer og beskriver de digitale sikkerhetsutfordringene knyttet til IKT-kriminalitet, spionasje, sabotasje og terror. Herunder foreslås en rekke tiltak som kan møte utfordringene på kort og lang sikt.[5]

[3]Se NOU 2015 nr. 13 - Kapittel 13.7.1, kapittel 14.7.3, kapittel 15.6.2, kapittel 17.7.1, kapittel 18.5.1, kapittel 23.4 herunder kapittel 23.4.2

[4] SFR s. 45 tiltak nr. 50

[5] Se NOU 2015 nr. 13 - særlig kapittel 21.11.1 – 21.11.4 og 21.11.8

2.2.1 Om et helhetlig rammeverk

NSM er enig i utvalgets anbefaling om at det må etableres et helhetlig rammeverk for å avklare og tydeliggjøre innsatsen mellom relevante aktører innen hendelseshåndtering. Utvalget uttaler at rammeverket må revideres og harmoniseres opp mot nasjonalt beredskapsplanverk.

Situasjonen i dag er at det finnes en rekke sikkerhetsregler, ordninger og beslutninger, både med sektorovergripende og sektoravgrenset rekkevidde, som har betydning for den samlede nasjonale evnen til å avdekke og håndtere digitale angrep. Denne fragmenterte situasjonen ble søkt avbøtet gjennom Nasjonal strategi for informasjonssikkerhet av 2012.

JD har i samarbeid med NSM utviklet et sett anbefalinger og retningslinjer for digital hendelseshåndtering for sivil side av samfunnet[6]. Forsvarsdepartementet (FD) har utviklet cyberretningslinjer for forsvarssektoren[7]. Disse bør danne utgangspunktet for det videre arbeidet med et helhetlig rammeverk. For EOS-tjenestenes samarbeid på dette feltet foreligger egne retningslinjer, som også må ses hen til.

NSM anbefaler at et forbedret rammeverk tar utgangspunkt i de initiativer som alt foreligger og de veivalg som er foretatt. Erfaringer fra øvelser må også trekkes inn i dette forberdringsarbeidet som bør ledes av JD og FD i samarbeid.

Etableringen av et forbedret nasjonalt rammeverk må ses i sammenheng med at det er mange pågående utrednings- og revisjonsprosesser som har betydning for digital hendelseshåndtering og deteksjon, ansvarsfordeling og nasjonal operativ evne.

2.2.2 Om økt nasjonal deteksjonsevne og felles situasjonsbilde

NSM er enig i utvalgets anbefaling om at informasjonsdeling i forbindelse med hendelser må starte tidligere enn det som er tilfellet i dag. Under kapittel 21.11.3 presiseres tiltaket i tre punkter. Herunder skriver utvalget i *punkt 1* at en hensiktsmessig teknisk plattform må på plass for å sørge for rask og sikker deling av ugradert informasjon fra NSM NorCERT.

NSM har gått inn i to nasjonale prosjekter som skal ta frem en sikker plattform for ugradert informasjonsdeling. Det ene prosjektet er i regi av Universitetet i Oslo (UiO). Det andre prosjektet, som skal ta frem en konkret løsning, er et samarbeidsprosjekt som er delvis finansiert av Forskningsrådet. Deltakere i dette prosjektet er NSM, UiO, Mnemonic, KraftCERT og FinansCERT.

Under *punkt 2* skriver utvalget om styrket deteksjonsevne gjennom tilpasset monitorering i den enkelte sektor. NSM støtter utvalgets forslag om at videreutviklingen bør skje i samarbeid med sektormyndighetene. Herunder forutsetter NSM at sektormyndighetene tar sterkere grep om eget sektorresponsmiljø slik at alle samfunnsviktige deler av sektoren blir ivaretatt.

Utvalget skriver i kapittel 21.5.1 om utfordringer knyttet til avdekking av sårbarheter og deteksjon av IKT-hendelser, herunder en utilstrekkelig nasjonal evne til å oppdage IKT-hendelser. VDI er i dag et av de viktigste verktøyene norske myndigheter har til å detektere og verifisere cyberangrep, herunder spionasje fra fremmede statlige aktører, mot norsk

[6] Modell for håndtering av IKT-sikkerhetshendelser - anbefalinger og retningslinjer, fra JD til departementene
[7] Retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren

infrastruktur. Dette har bidratt til at myndighetene har håndtert en betydelig mengde hendelser og avdekket flere alvorlige angrep mot norske bedrifter og myndigheter. En videreutvikling av løsningen vil gi norske myndigheter mulighet for å bygge opp en meget god deteksjonsevne på nasjonalt nivå. NSMs foreslåtte satsing på dette i SFR er i tråd med hvordan andre internasjonale samarbeidspartnere videreutvikler sine nasjonale kapasiteter.

NSM mener også at finansieringsordningen har betetydning for den nasjonale håndteringsevnen.

Hver VDI-deltager dekker kostnaden for egen sensor, mens NSM finansierer sentral infrastruktur samt utvikling og forvaltning.Private medlemmer i VDI betaler en deltakeravgift til NSM. Situasjonsbildet på internett er dermed avhengig av om viktige private selskaper ønsker å være med i samarbeidet eller ikke.

Deltakelse i VDI bør være basert på en risikovurdering, og behovet for å se dataangrep på tvers av sektorer, i motsetning til dagens ordning der systemet i stor grad finansieres av private aktører gjennom deltakeravgift. Dagens finansieringsmodell gir etter NSMs mening en ubalanse. Midler til VDI oppnås i praksis gjennom å øke privat deltakelse styrt av betalingsvilje, med den følgen at offentlige myndigheter kan bli underprioritert. På den måten kan fokus dreies vekk fra det reelle risikobildet. Finansieringsordningen er etter NSMs syn en sentral del av utfordringsbildet. NSM mener dagens sensornettverk (VDI) bør utvikles til å være fullfinansiert av staten. Det kan imidlertid tenkes alternative finansieringsmodeller. NSM mener dette isåfall bør være gjenstand for en nærmere utredning.

Antallet sensorer bør økes betydelig slik at utbredelsen av sensorer dekker det reelle risikobildet. Alternativt må sensorer plasseres sentralt hos for eksempel internettleverandører, for å gi en betydelig bedre deteksjonsevne ved samfunnsviktige funksjoner.

NSM mener at FDog JD bør ta initiativ til at deltakelse i VDI-samarbeidet fullfinansieres av staten. Dette er også foreslått i SFR.[8]

NSM mener videre det bør utredes en mulighet for å pålegge virksomheter med samfunnskritisk IKT-infrastruktur en deltakelse i VDI-samarbeidet. Ved en eventuell omlegging til fullfinansiering og pålagt deltakelse er det viktig at man søker å ta vare på de gode relasjonene som er opparbeidet mellom myndighetene og de private bidragsyterne.

NSM vil i denne sammenhengen også bemerke viktigheten av at evnen til å oppdage alvorlige IKT-hendelser er avhengig av at den totale nasjonale evnen til deteksjon bedres.

Det foreligger forslag fra henholdsvis Etterretningstjenesten og PST for å gi et legalgrunnlag for utvidet aktivitet i det digitale rom. Bakgrunnen for forslagene er den teknologiske utvikling og behovet for å håndtere risikoer som ellers hadde unndratt seg dette.

Det er viktig for et kosteffektivt forebyggende sårbarhetsreduserende sikkerhetsarbeid at man har best mulig kunnskap om hvilke trusler beskyttelsestiltakene skal virke opp i mot.

[8] SFR s. 44

For å unngå sikkerhetstruende hendelser er det også viktig at aktører med ansvar for trusselrettet forebygging og etterforsking har best mulig vilkår for å kunne lykkes med henholdsvis avskrekking, oppdagelse og iretteføring.

NSM mener på denne bakgrunn at forslagene er viktige og bør følges opp.

Utvalget har anbefalt en åpen og bred debatt knyttet til E-tjenestens og PSTs forslag[9]. Dette for å skape legitimitet. Denne utredningen er igangsatt, og NSM ser frem til resultatet.

Under *punkt 3* skriver utvalget at det bør etableres et felles situasjonsbilde som kan deles med sektorvise responsmiljøer og andre relevante aktører.

Det foreslås at Nasjonal kommunikasjonsmyndighet (Nkom) bør vurdere å etablere en automatisert prosess for informasjonsdeling om norske datamaskiner som er i bruk i digitale angrep mot norske telekomoperatører. NSM mener dette er en fornuftig tilnærming, da Nkoms ansvarsområde omfatter «intenett abuse» og direktoratet har nær forbindelse med norske internettleverandører.

Hva gjelder utvalgets forslag om å etablere et felles situasjonsbilde, mener NSM dette kan bygges videre på allerede etablerte oppdrag. NSM har allerede en oppgave om å ta frem et nasjonalt IKT-risikobilde som skal omfatte både statssikkerhet, samfunnssikkerhet og individsikkerhet. Et felles situasjonsbilde kan bygges på dette produktet. Dersom dette situasjonsbildet skal være noe mer, bør det utredes hvordan «produktene» kan virke sammen.

2.2.3 Om sektorvise responsmiljøer

NSM støtter som utgangspunkt utvalgets forslag om å evaluere ordningen med sektorvise responsmiljøer, omtalt i kapittel 21.11.4 punkt 1. NSM vil bemerke at selv om dette ble foreslått som tiltak i nasjonal informasjonssikkehetsstrategi i 2012, har implementeringen kommet kort. NSM antar at utvalgets øvrige forslag knyttet til sektormyndighetenes sterkere ansvar for eget håndteringsmiljø og en sterkere overordnet styring fra JD vil medføre at ordningen kan fungere etter intensjonen. NSM er av den klare oppfatning av at satsningen er riktig, men at prosessen og realiseringen av planen kan evalueres.

NSM viser til gjeldende Nasjonal strategi for informasjonssikkerhet og tilhørende handlingsplan hvor etableringen av sektorvise responsmiljøer er fremhevet som et viktig og prioritert tiltak som det skal arbeides systematisk for å etablere i de ulike sektorene. Samfunnets evne til å drive digital hendelseshåndtering krever stor grad av samarbeid både innad i den enkelte sektor og mellom sektorene. NSM er av den oppfatning at de sektorvise responsmiljøene bør ha en organisatorisk tilknytning til sektormyndigheten. NSM anser i den sammenheng fremveksten av responsmiljøer organisert som private rettssubjekter uten myndighetstilknytning som en utfordring. Erfaring tilsier at private medlemsfinansierte sektorresponsmiljøer vil dreie fokus til å håndtere kundekretsens umiddelbare behov og ikke nødvendighvis ta et helhetlig ansvar for sektoren. Kun gjennom myndighetsstyrte sektorresponsmiljøer vil sektorens totale infrastruktur gis en helhetlig dekningsrad. Dette vil igjen tjene samfunnets sikkerhetsinteresser på en bedre måte enn dersom private interesser er styrende for tilknytningen til et responsmiljø.

[9] NOU 2015 nr. 13 – Kapittel 21.11.8

Hensikten med etableringen er først og fremst at sektorresponsmiljøet skal ha evne og kompetanse til å dele informasjon om hendelser i egen sektor og fungere som et bindeledd mellom sektoren og NSM på nasjonalt nivå. For NSM er det viktig å ha slike miljøer som kontaktpunkt i den enkelte sektor. Sektorenes ulikhet tilsier at løsningene kan være noe forskjellige, prinsippet om myndighetstyring må imidlertid gjelde for alle.

NSM har en viktig rolle med å binde disse miljøene sammen, og koordinere aktiviteten. Miljøene bør på sikt kunne ha evne og kompetanse til å analysere informasjon om hendelser i sektoren. NSM må spille en rolle for å bidra til kompetansen i de sektorvise miljøene og gjøre dem i stand til å ivareta sin rolle på det operative nivået. NSM må håndtere grensesnittet mellom strategisk og operativt nivå og sørge for tilstrekkelig koordinering.

2.2.4 Om virksomhetenes evne

Utvalget foreslår under kapittel 21.11.1, 11 punkter som beskriver ambisjonsnivået for myndighetenes operative evne for å håndtere en alvorlige IKT-hendelser, mange av disse har fokus på virksomhetene.

Til *punkt 1* har NSM forhåpninger om at endringer i sikkerhetsloven vil medføre at det stilles krav til virksomhetenes evne til grunnleggende egenbeskyttelse, eventuelt at dette kan gjøres gjennom krav i eget sektorregelverk for den enkelte sektor basert på et felles samordnende rammeverk. NSM mener at problemstillingen bør drøftes i utvalget som skal foreslå nytt lovgrunnlag for forebyggende nasjonal sikkerhet.

Til *punkt 2 og 3* mener NSM at det er viktig at det etableres en gjensidig forståelse for viktigheten av å dele informasjon. Myndighetene bør dele så mye som mulig, men virksomhetene må også være i stand til å dele relevant hendelsesinformasjon med myndighetene og hverandre. Flere større konsern har vært åpne om IKT-hendelser i ettertid, noe som er bra og som bidrar til å sette fokus på hendelseshåndtering og deteksjon, men NSM anser likevel at det fremdeles er utfordringer knyttet til virksomhetenes vilje til å dele relevant informasjon med hverandre i IKT-hendelsenes tidligere faser. Det vises i denne forbindelse til nasjonale anbefalinger om åpenhet om IKT-hendelser.[10]

Til *punkt 5* er NSM enige i at myndighetene må være i stand til å bistå virksomhetene. Myndighetenes bistand til virksomhetene bør som utgangspunkt baseres på beredskapsprinsippet om nærhet, som vil tilsi at et godt etablert og utbygget sektororgan som regel vil stå nærmest til å gi virksomhetene bistand. Utfordringen er der hendelseshåndteringen er så kompetansemessig krevende eller håndteringen er en del av et større problemkompleks som kun kan løses på nasjonalt plan. NSM vil som det nasjonale responsmiljøet kunne tilby virksomhetene dybdeanalyse og bistand til hendelseshåndtering der skadepotensialet er alvorlig. Sektormyndighetene og sektorresponsmiljøet, som har oversikt over håndteringskapasiteten i egen sektor spiller en viktig rolle for at virksomhetene skal kunne settes i stand til å motta bistand fra NSM. NSM mener dette best kan gjøres ved å etablere myndighetsstyrte sektorresponsmiljøer underlagt et felles rammeverk.

Til *punkt 6* vil NSM bemerke at direktoratet har iverksatt et prosjekt som innebærer en godkjenningsordning av kommersielle hendelseshåndteringskapasiteter. Dette prosjektet evalueres fortløpende. NSM mener det bør utredes på hvilken måte myndighetene kan få nyttiggjøre seg av erfaringer kommersielle aktører tilordner seg gjennom sin håndtering.

[10] Nasjonale anbefalinger om åpenhet om IKT-hendelser, brev fra JD til departementene

Herunder vises til punkt 3, hvor det påpekes at informasjonsdeling tidlig i håndteringskjeden er viktig.

Til *punkt 8* viser NSM igjen til omtalen av å bygge opp sektorsystemet med detaljkunnskap om egen sektor, med en informasjonsdelingslinje opp til den nasjonalt koordinerende instansen i NSM NorCERT.

2.2.5 Nærmere om forbedring av nasjonal operativ evne gjennom samlokalisering

NSM er enig i utvalgets flertallsmerknad til kapittel 21.11.2. Videre er NSM enig i at det bør bygges videre på den eksiterende strukturen, at ambisjonspunktene som beskrevet i kapittel 21.11.1 må følges opp og at dette må gjøres gjennom styring fra JD, men i nært samarbeid med FD. NSM registerer at utvalget har et sammenfallende syn med NSM om at samlokalisering er et godt virkemiddel[11] enten det er en permanent løsning, en samling av enkelte aktører eller bruk av liasoner der det er mest hensiktsmessig.

NSM mener dette vil legge godt til rette for gjennomføringen av NSMs ansvar for koordinering av IKT-hendelser.

2.2.6 Nærmere om plassering av ansvaret for den nasjonale responskapasiteten

NSM registrerer at utvalget er delt i spørsmålet om plasseringen av den nasjonale responskapasiteten.

NSM mener flertallets løsning og begrunnelse for plassering er mer hensiktsmessig enn mindretalls forslag. Det vil være en bedre løsning å videreutvikle og se på handlingsrommet i eksisterende struktur for å overkomme delingsproblematikken, heller enn å etablere en ny struktur.

NSM er enig i at det kan fremstå som et spenningsfelt mellom rikets sikkerhet og sikkerhetsgradert informasjon på den ene siden, og samfunnets behov for åpenhet og informasjonsdeling på den andre siden. NSM er imidlertid av den oppfatning at det ikke trenger å være en motsetning mellom disse hensynene. EOS-miljøet og samarbeidspartnere tilfører håndterings- og avdekkiningsdimensjonen meget verdifull informasjon som kan omsettes i tiltak og komme resten av samfunnet til gode. Denne dimensjonen forsvinner dersom EOS-tjenestene ikke er premissleverandører for den totale nasjonale håndteringsevnen og CERT-funksjonen legges utenfor en av tjenestene. Per i dag har NSM en rekke arenaer der vi deler hendelsesinformasjon med eiere av kritisk infrastruktur, Forsvaret, politiet/Kripos, sentrale departementer og andre myndighetsorganer. NSM mener det er fullt mulig å dele informasjon med disse organene og likevel hensynta balansen mellom rikets sikkerhet på den ene siden og behovet for å dele med de nevnte organene på den andre siden. Delingsarenaene har et utviklingspotensiale, og NSM arbeider med dette.

Videre er NSM uenig med mindretallet i at "et nasjonalt cybersikkerhetssenter" bør legges til det ordinære politiet. NSM antar at mindretallet her ser for seg en løsning hvor dagens EOS-tjenester med NSM NorCERT i spissen skal inneha en GovCERT-rolle, og at Politiet iveratar den nasjonale CERT-funksjonen. NSM kan ikke se at dette forslaget vil løse de utfordringene utvalget beskriver. Mindretallet foreslår også en samlokalisering, men med et skille mellom

[11] SFR s. 43 tiltak nr.43

EOS-tjenestenes graderte hendelseshåndtering og samfunnssikkerhet generelt. Dette skillet vil tvert imot vanskeliggjøre at dimensjonene kan trekke veksler på hverandre.

Etter NSMs kunnskap finnes det ikke strukturer i andre land knyttet til håndtering av digitale sikkerhetstruende hendelser hvor politiet har det overordnede ansvaret. NSMs oppfatning er at politiet ikke har det tilstrekkelige handlingsrommet som en etat utenfor politiet har. NSM ser heller nytten av å styrke og videreutvikle et godt samarbeid mellom, virksomheter, sektorvise responsmiljøer, nasjonalt responsmiljø og politiet innenfor et helhetlig rammeverk for hendelseshåndtering.

Den norske modellen slik den er i dag, ses på som attraktiv av våre utenlandske samarbeidspartnere, og at det unike er at man har fått til et samarbeid mellom EOS-dimensjonen og virksomheter som eier samfunnskritisk infrastruktur. Tilliten som i dag er bygget opp mellom norske myndigheter og norsk næringsliv gjennom VDI over 15 år er unik i europeisk sammenheng. Disse samarbeidsrelasjonene vil neppe la seg videreføre hvis funksjonen skulle plasseres utenfor tjenestene.

2.2.7 Om behovet for en nasjonal cyberreserve

Utvalget skriver at JD og FD bør utrede en løsning med en såkalt «cyberreserve», omtalt i kapittel 21.11.4 punkt 2. NSM støtter utvalgets anbefaling. NSM mener at dette behovet må ta utgangspunkt i at strukturen (nasjonalt, i sektorene og i virksomhetene) i en normalsituasjon vil ha betydelige ressurser som forutsettes utnyttet på tvers innen rammen av en helhetlig nasjonal håndteringsplan.

2.3 Satellittbaserte tjenester

NSM er positive til at utvalget løfter frem tydeliggjøring av et myndighetsansvar for norsk romvirksomhet som en av de viktigste anbefalingene.

NSM merker seg at utvalget under kapittel 12.5.1 foreslår, *"å vurdere om det bør være et myndighetsorgan som får særskilt ansvar for å følge opp satellittbaserte tjenester på nasjonalt tverrsektorielt nivå"*. NSM mener dette bør ivaretas innen dagens struktur, fremfor å opprette et nytt organ. Det vil være mer kostnadseffektivt å gjennomgå dagens struktur for å kunne tilføre en nærmere angitt myndighet ytterligere kompetanse og ressurser for å kunne videreutvikle sitt ansvar og sin rolle. Ettersom det i dag er en rekke myndighetsorganer på området, støtter NSM utvalgets syn på at det må foretas en vurdering hvor ansvars- og rollefordeling gjennomgås. Under en gjennomgang bør det tas utgangspunkt i å beskrive "nåsituasjonen" av dagens forvaltningsregime, for å kartlegge hvilke områder som ikke er tilstrekkelig ivaretatt. Dette vil kunne danne et grunnlag for en bedre vurdering av hvilke myndighetsoppgaver som skal ivaretas av hvilket myndighetsorgan. Utvalget anbefaler at ansvaret enten legges til Nkom eller Direktoratet for samfunnssikkerhet og beredskap (DSB). NSM har gjennom flere år opparbeidet seg en betydelig kompetanse innenfor romvirksomhet, og har inngående kjennskap til prosjektet Galileo. NSM har gjennom tilsyn og arbeid med forebyggende sikkerhet en god forståelse for romvirksomhet, sårbarhetsaspekter og hvordan sårbarheter kan reduseres innenfor dette området. NSM bidrar i sikkerhetsarbeidet innen EU-programmet Galileo og har ansvar for sikkerhetsgodkjenning av de norske jordstasjonene.

NSM mener at den foreslåtte vurderingen bør foretas i samarbeid mellom relevante aktører, herunder Norsk Romsenter, NSM, Nkom og DSB.

2.4 Bruk av informasjonssystemer i krisesituasjoner

Utvalget peker i kapittel 20.1.2 på at hvert enkelt departement har primæransvaret for egne IKT-løsninger for å kunne opprettholde egen styring og kriseledelse. Utvalget ser det som viktig at det er i ferd med å utvikles et felles gradert system for sentralforvaltningen, men peker på at brukervennligheten for en del av de graderte systemene oppfattes som lav, og at det trenes for lite på å bruke dem, se kapittel 20.3.3. Dette kan etter utvalgets mening tale for en variantbegrensning, men at dette må vurderes opp mot de ulike behovene og den robustheten som ulike systemer gir.

NSMs oppfatning er at utvikling og forvaltning av et stort antall ulike systemer erfaringsmessig ikke bidrar til økt robusthet og sikkerhet. Utvikling av høygraderte systemer er ressurskrevende og krever spesiell kompetanse. Det er lite som tiliser at informasjonssystemer vil fungere bedre i krise eller krig enn de gjør i en normalsituasjon med alle ressurser tilgjengelig. NSM anbefaler i SFR at forsvarssektoren bør være den nasjonale leverandøren for å utvikle og forvalte løsninger for det høygraderte IKT-behovet i offentlig sektor, og at JD og FD bør ta initiativ til at det etableres felles IKT-systemer som håndterer sensitiv og BEGRENSET informajson.[12] [13]

NSM mener at JD og FD bør ta initiativ til å utrede løsninger for færre IKT-miljøer (utviklings- og forvaltningsorganisasjoner) i offentlig sektor, som det også fremgår av SFR[14], noe som vil gi stordriftsfordeler med mer robuste kompetansemiljøer og kostnadseffektive sikkerhetsløsninger. NSM mener JD bør stille krav om samordnede løsninger i sentralforvaltningen, for å bidra til en god tverrsektoriell samhandling både i normalsituasjoner og i krisesituasjoner. Herunder bør det gjennomføres årlige øvelser i IKT-sikkerhet og hendelseshåndtering. [15]

2.5 Utvikle felles beskyttelsestiltak mot sofistikerte digitale angrep

Utvalget beskriver i kapittel 22.6.2 et tiltak som går på å utvikle felles beskyttelsestiltak mot sofistikerte IKT-angrep, som skal tas i bruk i offentlig sektor. Herunder foreslår utvalget at Direktoratet for forvaltning og IKT (Difi) skal ha en koordinerende rolle, med bistand fra forskningsmiljø og NSM. Problemstillingen kan imidlertid ikke avgrenses til forvaltingen, men må sies å være er et nasjonalt anliggende, hvor næringsaktører har en betydelig rolle. Videre begås denne type angrep i det vesentlige av fremmede stater. Kunnskapen og komptansen om slike angrep ligger hos EOS-tjenestene. Utvikling av beskyttelsestiltak bør skje innen rammen av EOS-tjenestenes arbeid og ivaretas av NSM.

NSM har allerede rollen å koordinere arbeidet mellom andre myndigheter som har en rolle innenfor forebyggende IKT-sikkerhet. Til dette hører bl.a. koordinering av forskning og utvikling innen IKT-sikkerhet.[16]

2.6 Regulere elektronisk identitet

Utvalget beskriver i kapittel 22.6.3 flere tiltak knyttet til regulering av elektronisk identitet. Utvalget skriver under kapittelets punkt 2 at *«KMD bør utarbeide en tydelig definisjon av*

[12] SFR s. 39 tiltak nr. 24
[13] SFR s. 41 tiltak nr. 40
[14] SFR s. 40 tiltak nr. 25
[15] SFR s. 36 tiltak nr. 12
[16] Se Instruks for sjef Nasjonal sikkerhetsmyndighet, desember 2014

sikkerhetsnivåene. Den bør ta utgangspunkt i kombinasjoner av angriperens evne og konsekvens. Det må være enkelt å avgjøre om en e-ID når et sikkerhetsmål.» NSM mener at det er lettere å si noe om hvorvidt en konkret eID tilfredsstiller gitte sikkerhetskrav dersom man anvender anerkjente internasjonale sikkerhetsstandarder og profiler når kravene skal formuleres og når løsningen skal etterprøves. Common Criteria og ISO/IEC 15408 er internasjonalt anerkjente standarder. Både signaturfremstillingssystemene og selve chipen bør gjennomgå en uhildet tredjepartsvurdering i henhold til internasjonalt anerkjente standarder.

2.7 Nærmere om sertifisering

NSM mener at krav om sertifisering er et godt tiltak for bedre IKT-sikkerhet.

Utvalget skriver blant annet om digitale sårbarheter i kraftforsyningen, kapittel 13.5 side 126: *«Sentrale problemstillinger som diskuteres internasjonalt er krav til SCADA og AMS-sikkerhet, krav til godkjenning av systemer og krav til sertifisering.»* Det kan være verdt å se nærmere på noen av de erfaringene som sertifiseringsmyndighetene under CCRA har gjort når det gjelder muligheter for å bruke Common Criteria som sertifiseringsstandard for AMS og øvrige komponenter som inngår i smart-grid hvor det bør etableres formålstjenlige sikkerhetskrav.

Utvalget skriver i kapittel 21.2.1 side 257 at *«NSM utøver en rekke forebyggende myndighetsoppgaver etter sikkerhetsloven, som godkjenning av sikkerhetsgraderte informasjonssystemer, sertifisering av informasjonssystemer...»* Det er viktig å understreke at NSM også sertifiserer IKT-sikkerhetsfunksjonalitet og produkter ut over sikkerhetslovens ramme gjennom å forvalte Sertifiseringsmyndigheten for IT-sikkerhet (SERTIT). SERTIT bygger på de internasjonale arrangementene *"Arrangement of the Recognition of the Common Criteria Certificates in the field of Information Technology Security"* (CCRA) og *"Mutual Recognition Arrangement of Information Technology Security Evaluation Certificates"* (SOG IS MRA). Sertifisering av IKT-sikkerhet i regi av SERTIT er basert på en uhildet tredjepartsvurdering som også tilbys i det kommersielle markedet. Sertifikater gitt av SERTIT kan også benyttes som grunnlag for sertifisering i henhold til krav i medhold av sikkerhetsloven eller andre krav som må legges til grunn for IKT-sikkerhet.

2.8 Nærmere om Justis- og beredskapsdepartementets rolle

Utvalget beskriver JDs ansvarsområder flere steder i rapporten. I kapittel 23.3.1 foreslår utvalget en tydeliggjøring av JDs rolle, slik at det fremgår at JDs samordningsrolle gjelder både offentlig og privat sektor, herunder at det, om nødvendig, fremkommer av en revidert Kgl.res 22. mars 2013.

Mange ulike aktører, både departementer og etater, har koordinerende ansvar for et fagfelt. Dette kan være utfordrende innenfor rammene av konstitusjonelle ansvarsforhold, der den enkelte statsråd er ansvarlig innenfor sitt fagfelt. JDs koordinerende rolle innenfor forebyggende sikkerhet i sivil sektor er ikke i tilstrekkelig grad operasjonalisert slik at departementet kan ta sin rolle med den kraft som er nødvendig. En slik operasjonalisering er en forutsetning for dette. Rollen må anerkjennes av aktørene som skal bidra i koordineringen. I tillegg ser NSM at det mangler, eller er for dårlig utviklede, samvirkemekanismer på plass mellom aktørene. Dette gir en utilstrekkelig koordinering på området. Opplevde uklarheter på høyere nivå vil forplante seg nedover.

NSM støtter utvalgets forslag og viser i denne sammenheng til egen anbefaling gitt i SFR.[17]

NSM støtter også utvalgets forslag i kapittel 23.3.2 om å styrke JDs virkemidler. Utvalget legger frem flere forslag i rapporten som innebærer å utarbeide oversikter over digitale sårbarheter mv. NSM anbefaler at JD ser på muligheten til å videreutvikle og samordne flere av de produktene som allerede produseres på området

Hva gjelder utvalgets anbefaling, i kapittel 23.2.2, om oppfølging av prosessen rundt EUs NIS-direktiv, vil NSM bemerke at denne prosessen pågår og at NSM bistår departementet i dette arbeidet. NSM har tidligere fremsendt en skisse for hvordan dette kan gjennomføres i norsk rett.

2.9 Nærmere om utkontraktering av skytjenester

Utvalget beskriver i kapittel 23.7 tre alternative informasjonskategorier regjeringen må ta stilling til knyttet til utkontraktering av skytjenester. NSM vil her bemerke at denne inndelingen fremstår som fhensiktsmessig, men vil samtidig uttrykke at det til kategori 2, *"informasjon som kan lagres i utlandet, men som må kunne flyttes tilbake til Norge ved særlige behov og på bestemte vilkår"*, kan innebære flere usikkerhetsmomenter. NSM mener herunder at det bør tas høyde for situasjoner hvor det ikke lenger vil være mulig å flytte informasjonen hjem. Det bør tas høyde for hvorvidt informasjonen faktisk kan flyttes hjem fra en lokasjon med et politisk ustabilt klima eller i en nød- eller beredskapssituasjon og hvilke konsekvenser dette kan få for det politiske klimaet landende imellom.

2.10 Generelt om objektsikkerhet

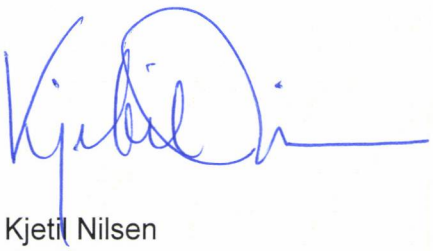
Utvalget har sammenfattet kunnskap og gitt en lang rekke anbefalinger som kan ha positiv innvirkning på arbeidet med identifisering og sikring av skjermingsverdige objekter innenfor sivil kritisk digital infrastruktur. I nasjonal strategi for informasjonssikkerhet (2012) står det at: *«Iverksettelse av endringene i sikkerhetslovens objektsikkerhetsbestemmelser er et viktig virkemiddel for å få identifisert samfunnskritiske funksjoner og avdekke innbyrdes avhengigheter mellom disse.[18]»* Et av strategiens sentrale tiltak for å styrke IKT-infrastrukturen er at: *«Fagdepartementene skal følge opp at sektorens virksomheter identifiserer og foreslår IKT-funksjoner og systemer som kan klassifiseres som samfunnskritiske i henhold til objektsikkerhetsregelverket.»*[19] Innenfor mange av de kritiske infrastrukturene utvalget omtaler er enkelte kjernenoder og IKT-systemer klassifisert som skjermingsverdige objekter i henhold til sikkerhetsloven, og underlagt tilsyn fra NSM eller relevant sektortilsyn, med hjemmel i sikkerhetsloven.

Utvalget skriver i kapittel 14.7.2 at *«Ingen av olje- og gassinstallasjonene er per i dag definert som skjermingsverdige objekter i henhold til sikkerhetsloven. [...]. I påvente av ny sikkerhetslov, samt eventuelle pålegg og direktiver fra EU, anbefaler utvalget at det settes i gang et arbeid med verdivurdering og klassifisering av anlegg og IKT-systemer.»* NSM støtter denne anbefalingen.

[17] SFR s. 35 tiltak nr. 1, 2, 3 og 4
[18] Nasjonal strategi for informasjonssikkerhet (2012) s. 18
[19] Nasjonal strategi for informasjonssikkerhet (2012) s. 18

NSM mener at problemet med uenighet om verdivurdering av skjermingsverdige objekter innenfor de ulike sektorer bør følges opp i forbindelse med det pågående arbeidet med ny sikkerhetslovgivning.

Med hilsen



Kjetil Nilsen
direktør