Rapport:
Evaluering av sektorvise responsmiljøer

Justis- og beredskapsdepartementet
Sak 21/6916

Juli 2022

www.kpmg.no

Sammendrag

På oppdrag for Justis- og beredskapsdepartementet (JD) har KPMG gjennomført en evaluering av ordningen med sektorvise responsmiljøer (SRM). Formålet med evalueringen er å bidra til JDs og Nasjonal sikkerhetsmyndighets (NSM) beslutningsgrunnlag for den videre utviklingen av SRM-ordningen.

Vi vil benytte anledningen til å takke alle de engasjerte og kunnskapsrike medarbeiderne i SRM-ordningen som har tatt seg tid og stilt opp. Dette har bidratt til å gi oss viktig innsikt i ordningens virkemåte. Vi vil også takke JD for en god og konstruktiv dialog gjennom hele prosjektperioden.

Bakgrunn

Etableringen av SRM i Norge har blant annet sitt utspring i Nasjonal strategi for informasjonssikkerhet (2012). I 2017 kom den første stortingsmeldingen om IKT-sikkerhet «IKT-sikkerhet – Et felles ansvar», der styrking av den nasjonale evnen til å avdekke og håndtere digitale angrep var et av hovedområdene. For å understøtte sektorene og virksomhetene i deres arbeid med å etablere responsmiljøer, og for å klargjøre forholdet mellom virksomhet, SRM og det nasjonale responsmiljøet hos NSM, ble det i 2017 gitt ut et Rammeverk for håndtering av IKT-sikkerhetshendelser. Rammeverket legger til grunn at SRM skal ha en sentral rolle i hendelseshåndteringen. En rekke sektorer har utpekt SRM, men det er stor variasjon i modenhet, omfang, kompetanse og innretning mellom SRM.

Sentrale observasjoner

KPMGs overordnede inntrykk gjennom evalueringsoppdraget er at samarbeidet mellom de ulike aktørene fungerer godt, det er god utveksling av informasjon, metoder, erfaringer og kompetanse på tvers av miljøene, og at ordningen med SRM har gitt et mer samlet cybersikkerhetsmiljø i Norge.

Gjennom dokumentanalyse, spørreundersøkelse og intervjuer har KPMG identifisert flere utfordringer i dagens ordning:

- ✓ Ulikheter i organisering og virkemåte kan føre til at det oppstår gap og uklare grensesnitt, og hvor enkelte sektorer og/eller virksomheter ikke dekkes tydelig av et SRM
- ✓ Det er ulike tolkninger av hvorvidt føringer gitt i rammeverket er krav eller veiledende
- ✓ Det er et gap mellom cybersikkerhetsområdets sektorovergripende natur og sektorprinsippet i staten
- ✓ Det fremkommer ikke i rammeverket hvilken rolle private leverandører av IKT-infrastruktur og andre samfunnsviktige tjenester skal ha i den overordnede modellen
- ✓ Et utfordrende rekrutteringsmarked og begrenset tilgang på relevant kompetanse
- ✓ Det er uklarheter knyttet til rolle- og ansvarsfordelingen i hendelseshåndtering

KPMGs anbefalte prinsipper for videreutvikling

KPMG foreslår et sett med prinsipper med formål om å styrke nasjonal evne til å avdekke og håndtere hendelser:

1. Rammeverket bør i større grad inkludere forebyggende arbeid med IKT-sikkerhet i tillegg til operative aktiviteter innen hendelseshåndtering
2. Den nasjonale innsatsen bør kraftsamles for å sikre grunnleggende nasjonale funksjoner
3. Spesifikke sektorvise behov skal ligge til grunn for opprettelsen av SRM

4. Det bør etableres formelle minimumskrav for et utpekt SRM
5. De ulike aktørenes rolle i hendelseshåndteringen bør nyanseres og tydeliggjøres

Forslag til videreutvikling av ordningen med sektorvise responsmiljøer

Formålet med forslagene til videreutvikling av dagens ordning med SRM er å nyansere ordningen og gjøre den mer behovstilpasset. Dette innebærer å bevege seg fra like krav og forventninger til alle sektorer og SRM, til å tillate ulike løsninger basert på om det er behov for en sektorspesifikk funksjon.

Det anbefales å stille ulike nivå av krav til responsmiljøene og samhandlingen mellom dem og sikkerhetsmyndigheten basert på følgende:

- ✓ hvor kritisk tilhørende virksomheter er for den nasjonale sikkerheten, og følgelig
- ✓ hvor omfattende konsekvenser en IKT-sikkerhetshendelse i disse virksomhetene vil få

Ettersom det pågår et arbeid i departementene med å identifisere grunnleggende nasjonale funksjoner og virksomheter som har vesentlig eller avgjørende betydning for disse, anbefales det å knytte nivåene i SRM-ordningen til dette arbeidet.

Det foreslås en tre-nivå modell der samhandlingsnivået og minimumskravene øker med virksomhetenes betydning for grunnleggende nasjonale funksjoner. Det er viktig å påpeke at forslaget utgjør et minimumsnivå, og at et SRM står fritt til å tilby ytterligere tjenester til sektoren der man vurderer dette som hensiktsmessig.

Nivå 0 – Basisnivå

Formålet med basisnivået er å sikre at varsling innenfor alle sektorer blir ivaretatt, og at alle virksomheter har tilgang til generell kunnskapsdeling i form av veiledere og annen generell rådgivning fra NSM. Dette nivået er et minimumsnivå som gjelder for alle sektorer, og bør dekke alle virksomheter uavhengig av tilknytning til SRM.

Nivå 1 – Vesentlig betydning

Formålet med nivå 1 er å sikre sektorspesifikk kompetanse i forbyggende og operativ IKT-sikkerhet i sektorer med virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner (GNF) eller av andre grunner har behov for sektorspesifikk kompetanse og koordinering.

På dette nivået er det utpekt et SRM av departementet. Disse skal oppfylle et sett med minimumskrav for dette nivået. For å sikre at SRM har nok kapasitet og kompetanse til å ivareta minimumskravene kan ulike departementer velge å samarbeide om en funksjon, spesielt i sektorer med begrenset rolle i samfunnskritiske funksjoner.

Nivå 2 – Avgjørende betydning

Formålet med nivå 2 er å styrke det forebyggende og operative samarbeidet på tvers av sektorer for å sikre samfunnets viktigste funksjoner.

Offentlige og private virksomheter som har avgjørende betydning i å understøtte grunnleggende nasjonale funksjoner bør inngå i en slik samarbeidsstruktur sammen med NSM og tilhørende SRM, der det er tett samhandling mellom aktørene på alle områder i hendelseshåndteringen.

Innholdsfortegnelse

1 Innledning

I dette kapittelet gir vi kort rede for bakgrunnen for oppdraget, problemstillinger og formål. Videre beskrives oppdragets metodiske tilnærming, begrepsbruk og definisjoner. Avslutningsvis presenteres rapportens struktur og videre oppbygging.

1.1 Bakgrunn

Etableringen av sektorvise responsmiljøer (SRM) i Norge har blant annet sitt utspring i Nasjonal strategi for informasjonssikkerhet (2012). Behovet for SRM ble aktualisert i august 2014 da det for første gang ble oppdaget at Norge var utsatt for et målrettet digitalt angrep mot en hel sektor. Om lag 50 bedrifter i olje- og energisektoren mottok én eller flere e-poster med skadevare. Omfanget av angrepet var uavklart, og Nasjonal sikkerhetsmyndighet (NSM) valgte derfor å varsle hele sektoren, totalt 300 bedrifter. Arbeidet med denne brede varslingen avdekket at man på nasjonalt nivå ikke hadde nødvendig oversikt over ulike sektorer. Basert på anbefaling fra NSM utarbeidet Justis- og beredskapsdepartementet (JD) "Modell for håndtering av IKT-sikkerhetshendelser – anbefalinger og retningslinjer" i 2014.

Parallelt arbeidet Lysneutvalget med utredningen «Digital sårbarhet – Sikkert samfunn» som ble lagt frem i november 2015. Utvalget ble nedsatt for å kartlegge samfunnets digitale sårbarhet. I utredningen ble det gjentatte ganger påpekt et behov for en sektortilnærming, uten at utvalget hadde det nødvendige grunnlaget for å vurdere i hvilken grad modellen var hensiktsmessig og innført i tråd med anbefalingene.

I 2017 kom den første stortingsmelding om IKT-sikkerhet «IKT-sikkerhet – Et felles ansvar», der styrking av den nasjonale evnen til å avdekke og håndtere digitale angrep var et av hovedområdene. Et sentralt tiltak for å bidra til en slik styrking var etableringen av et rammeverk for håndtering av IKT-sikkerhetshendelser. Som en følge av dette ble også ordningen med sektorvise responsmiljøer etablert. Responsmiljøene skulle ha oversikt i egen sektor, være informasjonsknutepunkt for alle relevante virksomheter og være sektorens bindeledd mot NSM. Et utkast til rammeverk ble benyttet under den nasjonale øvelsen IKT-16, slik at erfaringer fra øvelsen kunne benyttes i arbeidet med å ferdigstille rammeverket.

Rammeverk for håndtering av IKT-sikkerhetshendelser ble fastsatt av JD og Forsvarsdepartementet (FD) i desember 2017 og sendt ut til departementene for implementering innenfor de respektive forvaltningsområdene.

I 2018 leverte IKT-sikkerhetsutvalget en rapport der mandat og organisering innen IKT-sikkerhet var vurdert. Som en del av dette arbeidet så man på i hvilken grad rammeverket var innført i tråd med intensjonen og om man hadde oppnådd ønsket effekt. Et funn var at flere sektorer ikke hadde etablert egne responsmiljøer. Manglende finansiering, begrenset tilgang på relevant kompetanse og at ikke alle virksomheter hadde naturlig tilhørighet i en sektor ble trukket frem som mulige årsaker.

1.2 Problemstillinger og formål

Etter noen års erfaring med ordningen med sektorvise responsmiljøer ønsker JD å gjennomføre en ekstern evaluering av ordningen. Formålet med evalueringen er å bidra til JDs og NSMs beslutningsgrunnlag for den videre utviklingen av ordningen med sektorvise responsmiljøer.

Følgende formål og problemstillinger er satt for evalueringen:

- ✓ Kartlegge utfordringer i den nasjonale modellen for håndtering av IKT-sikkerhetshendelser slik denne er beskrevet i Rammeverk for håndtering av IKT-sikkerhetshendelser, med særlig vekt på sektorvise responsmiljøer.
- ✓ Vurdere hvordan ordningen med sektorvise responsmiljøer kan forbedres og anbefale tiltak for videreutvikling, herunder:
    - fordeling av ansvar og oppgaver mellom responsmiljøer på sektornivå og den nasjonale responsfunksjonen i Nasjonal sikkerhetsmyndighet, herunder informasjonsdeling på tvers og mellom nivåer
    - om kompetanse og kapasitet i større grad bør kraftsamles
    - om det er behov for et sett med formelle minimumskrav og kriterier for et sektorvis responsmiljø, f.eks. plikt til informasjonsdeling og varsel om hendelser, og formell utpeking fra et departement
    - forholdet mellom en myndighet og et utpekt sektorvis responsmiljø, som ikke er en del av myndigheten
    - hvordan responsfunksjonene kan utøves for virksomheter som ikke naturlig hører inn under en sektor eller som kan omfattes av flere sektorer
    - om det er alternative former for samarbeid i og mellom sektorer, særlig for å omfatte alle offentlige og private virksomheter som har betydning for kritisk infrastruktur og/eller kritiske samfunnsfunksjoner
    - hvilken rolle private aktører kan ha i den nasjonale responsmiljøstrukturen
- ✓ Vurdere de økonomiske og administrative konsekvensene av tiltak som anbefales.

Resultatet av evalueringen er sammenfattet i denne rapporten, og inkluderer både en beskrivelse av dagens situasjon og utfordringer i ordningen så langt.

1.3 Metodisk tilnærming

For å besvare problemstillingene har KPMG valgt en tilnærming som er basert på analyse av dokumenter, en spørreundersøkelse sendt til alle SRM og semi-strukturerte intervjuer med et utvalg SRM og andre interessenter. Det har underveis i prosjektet blitt gjennomført jevnlige møter med JD. Avslutningsvis ble det også gjennomført en workshop med representanter fra SRM. Workshopen var viktig for å innhente synspunkter på våre konklusjoner, vurderinger og anbefalinger. Workshopen har også vært viktig for å forankre rapporten i aktuelle, berørte miljøer.

1.3.1 Metode og datagrunnlag

Det er gjennomført en omfattende analyse av dokumenter som et ledd i arbeidet med rapporten. Sentrale, styrende dokumenter som belyser organiseringen av SRM er gjennomgått, herunder Rammeverk for håndtering av IKT-sikkerhetshendelser, ulike stortingsmeldinger og utredninger. Dernest har det blitt samlet inn en rekke rutiner og annen styringsdokumentasjon fra SRM som har blitt undersøkt. I de fleste tilfeller lyktes KPMG med å samle inn dokumentene før spørreundersøkelse og intervjuguider ble utferdiget. I så måte har dokumentene hatt en særlig sentral plass i det innledende arbeidet med å spesifisere undersøkelsesdesign og i den innledende fasen i forbindelse med utarbeidelse av spørreundersøkelse og intervjuguide. Samtidig har dokumentene også blitt benyttet til å verifisere og kontrollere opplysninger fra intervjuene der dokumentene inneholder informasjon som kan sees i lys av disse. På denne måten har dokumentene også vært benyttet for å kvalitetssikre informasjon fra intervjuer og observasjoner i spørreundersøkelsen.

Spørreundersøkelsen ble distribuert til samtlige SRM. Spørreundersøkelsen er i denne evalueringen et metodisk grep for å kartlegge bredt og skaffe oversikt over SRM på et overordnet nivå. Informasjonen i spørreundersøkelsen bidrar i hovedsak med å gi et helhetlig bilde over status og oppfatninger om SRM-ordningen i det brede lag av SRM.

KPMG har i arbeidet med evalueringen gjennomført intervjuer med et utvalg SRM i forskjellige sektorer. Intervjuobjektene har primært vært ledere i SRM-er, men i enkelte intervjuer har også operative rådgivere/fagpersoner vært med. KPMG har også deltatt i et møte med Nettverk for digital sikkerhet for å samle innspill fra representantene i departementene. I tillegg har det blitt gjennomført intervjuer med andre interessenter og fagpersoner som har bidratt med f.eks. styringsperspektiver eller input til erfaringer fra andre land. Videre er det avholdt flere intervjuer med NSM, og andre private og offentlige virksomheter med en sentral rolle i ordningen. Utvalget er gjort i dialog med JD. Intervjuene har gått i dybden på problemstillingene og forsøkt å belyse hvorfor det er sider ved rammeverket og ordningen som oppleves utfordrende/mindre relevant samt hva som kan gjøres for å styrke det. Det har også vært vektlagt å forstå samarbeidsmønstre opp mot medlemmer, andre SRM, myndighetene og andre sentrale interessenter. Der spørreundersøkelsen har gitt oversikt på et overordnet nivå bidrar intervjuene til at evalueringen i større grad går i dybden. Fullstendig oversikt over informanter og gjennomførte intervjuer er inntatt som vedlegg 2.

Før ferdigstilling av rapporten ble det gjennomført en workshop med flere SRM som har deltatt i prosjektet gjennom intervju og spørreundersøkelse. Formålet med workshopen var å gå ytterligere i dybden av funn som har framkommet med de øvrige metodene, bidra til å vurdere økonomiske og administrative konsekvenser og ellers korrigere eventuelle mangler og misforståelser. Det var videre et mål at workshopen skulle gi prosjektteamet et godt grunnlag for å ytterligere spisse våre vurderinger og anbefalinger.

Observasjonene fra dokumenter, spørreundersøkelsen og intervjuene, ble gruppert etter temaer relatert til gjennomgangens problemstillinger i et analyseskjema, som utgjør grunnlaget for rapporten. De sammenstilte observasjonene ga videre grunnlag for å identifisere anbefalinger om mulige tiltak som kan vurderes iverksatt. Observasjoner og foreløpige anbefalinger ble deretter presentert og diskutert i den nevnte workshopen.

Utredningsinstruksen har ligget til grunn for evalueringen. Dette innebærer at KPMG, ut fra tilgjengelig informasjon, har gjort vurderinger av de økonomiske og administrative konsekvensene av forslag til anbefalinger og alternative modeller/forslag til tiltak som har blitt tilrettelagt som et ledd i evalueringen. Videre har det i gjennomføringen blitt lagt vekt på minimumskravene til utredning som beskrevet i utredningsinstruksen.

1.3.2 Forbehold

Rapporten er utarbeidet på bakgrunn av de opplysninger som er gitt og den dokumentasjonen som har vært gjort tilgjengelig for KPMG. KPMG fraskriver seg ethvert ansvar for mulige feil eller utelatelser som følge av at det har blitt gitt uriktige eller ufullstendige opplysninger eller dokumentasjon.

Evalueringen og forslag til videreutvikling fokuserer kun på aktørene innenfor ordningen med SRM. Alle aktører i ordningen har i tillegg andre samarbeidspartnere, leverandører, kilder og kanaler til situasjonsbilde og informasjon mv., men de inkluderes ikke i denne evalueringen.

KPMG har undersøkt et stort og komplekst område med relativt kort gjennomføringstid. Vi mener likevel at rapporten belyser status for SRM-ordningen og gir konkrete forslag til anbefalinger for JDs videre oppfølging og forbedringsarbeid hva gjelder SRM-ordningen.

Følgende problemstillinger er blitt identifisert, men ikke inkludert i evalueringsoppdraget og forslag til videreutvikling av ordningen med SRM:

- ✓ Nasjonal deteksjonsevne er ikke berørt i rapporten. I hvilken grad dagens juridiske rammer og teknologisk løsninger muliggjør en effektiv nasjonal deteksjonsevne bør utredes videre.
- ✓ Felles samhandlingsplattform for SRM. Forenkling av dagens løsning med mange ulike kanaler kan bidra til enda mer effektiv samarbeid og informasjonsdeling.
- ✓ Felles modell for klassifisering av informasjon. Rapporten nevner kort enkelte utfordringer knyttet til bruk av Traffic Light Protocol (TLP).

- ✓ De fleste norske virksomheter har utarbeidet planverk og motstandsdyktighet i sine IKT-systemer for å detektere og håndtere hendelser i fredstid. Det kan være hensiktsmessig å se nærmere på tiltak, robusthet og beredskap i hele krisespennet samt definere grensesnitt mot Nasjonalt beredskapssystem.
- ✓ Et eventuelt behov for å etablere et «felles-SRM» under departement eller NSM for sektorer som ikke alene har behov for og/eller ressurser til et fullverdig SRM i sin sektor, men har behov for mer enn bare varsling og generell kunnskapsdeling.
- ✓ Forholdet mellom NIS 2 -direktivet og prosessen med å identifisere GNF (se vedlegg 3)

1.4 Begrep og definisjoner

Begrep	Forklaring
IKT-sikkerhetshendelse	«Tilsiktede uønskede hendelser eller trusler om slike hendelser i det digitale rom som er rettet mot kritisk infrastruktur og /eller kritiske samfunnsfunksjoner» (NSM, 2017).
Håndtering av IKT-sikkerhetshendelse / Hendelseshåndtering	«Defensive prosesser og tiltak for å detektere (avdekke) og stanse alvorlige IKT-sikkerhetshendelser, samt å gjenopprette sikker tilstand for berørte systemer, skadevurdere og skadebegrense» (NSM, 2019)
Sektorvis responsmiljø (SRM)	Et sektorvis responsmiljø er en IKT-sikkerhetsfunksjon som skal kunne bistå sin respektive sektor med kompetanse innen operativ IKT-sikkerhet og samtidig være knutepunkt for informasjon og informasjonsflyt mellom virksomheter i sektoren, mellom sektorer og mellom sektor og nasjonalt nivå.
IKT-sikkerhet / digital sikkerhet	«… at digitale tjenester og produkter er sikre og pålitelige fra starten, og i hele tjenestens eller produktets levetid» (Regjeringen, 2019).
Operativ IKT-sikkerhet	Operativ IKT-sikkerhet er en sikkerhetsdisiplin som kombinerer mennesker, teknologi og prosesser for å avdekke og håndtere trusler og sårbarheter i IKT-domenet. Operativ IKT-sikkerhet har til hensikt å forhindre, detektere, analysere og respondere på IKT-sikkerhetshendelser.
Kritisk infrastruktur	De anlegg og systemer som er nødvendige for å opprettholde samfunnets kritiske funksjoner som dekker samfunnets grunnleggende behov og befolkningens trygghet.
CERT	«Computer Emergency Response Team» er en koordinerende enhet for IKT-sikkerhet. CERT er en lisensbelagttittel. I Norge eksisterer ulike CERT-miljøer. NorCERT er det nasjonale CERT-miljøet. Se også CSIRT.
CSIRT	«Computer Security Incident Response Team" er en koordinerende enhet for IKT-sikkerhet. CSIRT er ikke en lisensbelagt tittel.
Trussel	«Mulig uønsket handling som kan gi negativ konsekvens for en entitets sikkerhet» (NS 5830:2012, s. 4).

Sårbarhet	«Manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning» (NS 5830:2012, s. 5).
Trusselaktør	En kjent eller ukjent aktør (person, organisasjon, land eller annen) som forbindes med en trussel. (NS 5830:2012)
Virksomhet	Betegnelse for en organisatorisk enhet som eksempelvis kan være et departement, et direktorat, en etat, en organisasjon eller et privat foretak. For dette rammeverket må det skilles mellom departementet som sekretariat for politisk ledelse, departementet som en virksomhet som skal ivareta egen sikkerhet, og departementet som overordnet ansvarlig for sikkerhet i egen sektor.
Grunnleggende nasjonal funksjon, GNF	Tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.
Varsling	Med varsling menes initiell rapportering av digitale hendelser, datainnbrudd, eller nylig oppdagede sårbarheter. Varsling innebærer informasjonsoverføring til en eller flere parter.
Rapportering	Med rapportering menes forløpende/jevnlig informasjons-overføring mellom to eller flere parter for å skape situasjons-forståelse. Rapportering knyttes til overføring av informasjon relatert til hendelser, potensielle trusler, sårbarheter eller annen relevant informasjon som bidrar til situasjonsforståelse.
Rammeverk for håndtering av IKT-sikkerhetshendelser, «rammeverket»	Rammeverk for håndtering av IKT-sikkerhetshendelser beskriver en systematisk tilnærming til håndtering av IKT-sikkerhetshendelser på tvers av virksomheter og sektorer for å sikre en effektiv nasjonal sektorovergripende håndteringsevne, hvor det enkelte departements konstitusjonelle ansvar også ivaretas. Siste versjon av rammeverket ble utgitt 07.12.17 av NSM. Rammeverket erstattet "Modell for håndtering av IKT-hendelser" utgitt av Justis -og beredskapsdepartementet i 2014.

Tabell 1 Begrep og definisjoner brukt i rapporten

1.5 Rapportens videre oppbygging

Rapporten er videre delt inn i ytterligere tre kapitler i tråd med de overordnede temaområdene for denne analysen.

I kapittel 2 redegjøres det kort for SRM-ordningen og de SRM som er inkludert i evalueringen.

I kapittel 3 gjøres det rede for observerte utfordringer knyttet til rammeverket og dagens ordning, herunder utfordringer opplevd av aktørene som inngår i rammeverket. Beskrivelsen av de opplevde utfordringene peker på mulige forbedringsområder og er følgelig et viktig grunnlag for å definere hva som ønskes oppnådd for derigjennom å skissere ulike tiltak. Siste del av kapittelet presenterer KPMGs vurderinger av utfordringene og skisserer noen prinsipper som KPMG mener det vil være hensiktsmessig å legge til grunn for det videre arbeidet med utviklingen av ordningen med sektorvise responsmiljøer.

I kapittel 4 presenteres våre anbefalinger, i form av en ny mulig modell. KPMG vurderer mulige virkninger av tiltakene, begrunner hvorfor KPMG anbefaler tiltakene og skisserer hvem som blir berørt og på hvilken måte.

2 SRM: Organisering og virkemåte

2.1 Om SRM-ordningen og rammeverk

Rammeverk for håndtering av IKT-sikkerhetshendelser

NSM beskriver at hensikten med rammeverket er å avklare og tydeliggjøre innsatsen mellom relevante aktører for å være bedre i stand til å håndtere alvorlige IKT-sikkerhetshendelser som rammer på tvers av sektorer. Videre skal det bidra til å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon om alle relevante IKT-sikkerhetshendelser.

Rammeverket bygger på tre aktørnivåer; virksomheter/systemeiere, sektorvise responsmiljøer og NSM. Det er således lagt opp til at SRM har en sentral rolle i håndteringen av IKT-sikkerhetshendelser. For hvert av aktørnivåene stilles det en rekke forventninger og krav knyttet til hvert av prosesstegene i rammeverket.

Sektorvise responsmiljøer

Etablering av sektorvise responsmiljøer er omtalt i stortingsmeldingen «Samfunnssikkerhet» fra 2012, der det står at «som en minimumsløsning skal det etableres et kontaktpunkt i sektoren for alvorlige IKT-hendelser og prosedyrer for varsling internt i sektoren og opp mot NorCERT[1]". Utover dette må sektorene selv vurdere hva slags behov de har for å håndtere IKT-kriser og hvordan de eventuelt skal skalere opp sine responsmiljøer.» Ordningen omtales også i Nasjonal strategi for informasjonssikkerhet fra 2012, og senest i nasjonal strategi for digital sikkerhet fra 2019. Der står det beskrevet at «Ambisjonen med de sektorvise responsmiljøene er at disse skal kunne bistå sin sektor med kompetanse og være knutepunkt for informasjon og informasjonsflyt mellom virksomheter i sektoren, mellom sektorer og mellom sektor og nasjonalt nivå (NorCERT).»[2]

I «Rammeverk for håndtering av IKT-sikkerhetshendelser (2017)» står det at det er departementenes oppgave å påse at det er etablert sektorvise responsmiljøer med et operativt ansvar for å dekke virksomheter innen hele eller deler av departementets myndighetsområde. Frem til et slikt miljø er etablert er det departementet selv som må ivareta oppgavene som ligger til SRM slik som beskrevet i rammeverket. Rammeverket oppgir videre en rekke oppgaver som tillegges de sektorvise responsmiljøene i forbindelse med håndtering av IKT-sikkerhetshendelser.

Det enkelte departementet har stor fleksibilitet knyttet til å vurdere hvorvidt det er hensiktsmessig med ett eller flere SRM i egen sektor.

[1] Nå Nasjonalt Cybersikkerhetssenter (NCSC)

[2] Tiltaksoversikt, Nasjonal strategi for digital sikkerhet (2019), https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

2.2 SRM inkludert i evalueringen

Følgende etablerte SRM er inkludert i evalueringen:

Navn	Overordnet departement	Årsverk	Finansiering	Dekningsområde	Formelt utpekt
JustisCERT	Justis- og beredskapsdepartementet (JD)	< 5	Over statsbudsjett	Hele sektoren	Etablert på oppdrag fra departement i 2012
HelseCERT	Helse- og omsorgsdepartementet (HOD)	>10	Hovedsakelig gjennom statsbudsjett, betalt monitorering i spesialisthelsetjenesten	Hele sektoren	Etablert av departement i 2011
NFCERT	Finansdepartementet (FIN)	>10	Medlemsavgift	Virksomheter som velger medlemskap. NFCERT operer i alle nordiske land (FI, DK, IS, NO, SE)	Forening etablert i 2013. Samarbeider med Finanstilsynet, som formelt er utpekt SRM.
KraftCERT	Olje- og energidepartementet (OED)	>10	Medlemsavgift, samt over statsbudsjett for varsling til ikke-medlemmer	Virksomheter som velger medlemskap, i tillegg til at ikke-medlemmer mottar varsler	Etablert av Statkraft, Statnett og Hafslund i 2014 etter initiativ fra NorCERT og NVE. NVE er formelt utpekt som SRM.
MiljøCERT	Klima- og miljødepartementet (KLD)	< 5	Over statsbudsjett	Direkte underliggende etater	Etablert på oppdrag fra departement
CSS/MilCERT	Forsvarsdepartementet (FD)	N/A	Over statsbudsjett	Forsvarsektoren med enkelte unntak	Forsvaret utpekt av FD. Etablert i Cyberforsvaret på oppdrag fra Forsvarssjefen.
DSS CERT	Kommunal- og distriktsdepartementet (KDD)	< 5	Over statsbudsjett (bevilgningsfinansiert over rammene til DSS).	Alle departementer unntatt FD, JD og UD. Visse andre organisasjoner, slik som Regjeringsadvokaten.	Startet som team for operativ sikkerhet i 2009. Re-etablert som DSS CERT i 2016. Er del av driftsmiljøet for departementenes felles IKT-løsning hos DSS.
Landbruks- og matCERT	Landbruks- og matdepartementet (LMD)	< 5	Over statsbudsjett.	Direkte underliggende etater	Etablert og driftet av Landbruksdirektoratet på oppdrag fra departement.
EkomCERT	Kommunal- og distriktsdepartementet (KDD)	< 5	Over Nkom sine budsjetter. Disse består hovedsakelig av lisenser/sektoravgifter som betales av norske ekomtilbydere.	Alle virksomheter som defineres som ekomtilbydere. Ca. 130 virksomheter har gitt kontaktinformasjon og mottar dermed varsler og informasjon.	Arbeidet med å kartlegge behov og lage kravspesifikasjon for SRM startet i 2015. Operasjonalisert i 2017, etter ett års testing.
eduCSC (tidligere Uninett CERT)	Kunnskapsdepartementet	6 – 10	Gjennom sentrale satsningsmidler og brukerbetaling i perioden 2019-2022. Fra 2023 vil de sannsynligvis kun være finansiert av brukerbetaling.	SRM for høyere utdanning og forskning. Leverandør av sikkerhetstjenester for hele kunnskapssektoren. Dagens kunder er i hovedsak utdanningsinstitusjoner og forskningsinstitutter.	Formelt utpekt som SRM av Unit på vegne av KD i 2020. Forløperen til eduCSC, Uninett CERT har eksistert siden 90-tallet.
Kommune-CSIRT	N/A (IKS, Gjøvik og Lillehammer kommune)	1 – 5	Medlemsavgift	Kommuner som velger medlemskap	Etablert og eid av Gjøvik kommune og Lillehammer kommune. Ikke utpekt som SRM av departementet, men deltar SRM-ordningen etter avtale med NSM.

Tabell 2 Sektorvise responsmiljøer i evalueringen

3 Utfordringer i dagens ordning og KPMGs vurderinger

Gjennom dokumentanalyse, spørreundersøkelse og intervjuer har KPMG identifisert en rekke utfordringer i dagens ordning. Dette kapittel beskriver de identifiserte utfordringene samt KPMGs vurderinger. Kapittelet er strukturert i følgende temaer:

- ✓ Organisering, ansvarsfordeling og virkemåte
- ✓ Sektorprinsippet
- ✓ Kompetanse og kapasitet
- ✓ Private aktørers rolle
- ✓ Kommunikasjon og samarbeid

Basert på vurderingene anbefaler KPMG fem prinsipper for videreutvikling av ordningen med sektorvise responsmiljøer. Disse presenteres i slutten av kapitlet.

3.1 Store variasjoner i organisering, ansvarsfordeling og virkemåte

Vårt overordnede inntrykk er at de sektorvise responsmiljøene er svært forskjellige i måten de er organisert på, hvilke oppgaver de gjennomfører for sitt departement og hvilket dekningsområde de har i sin sektor. Det er identifisert flere utfordringer knyttet til organisering, ansvarsfordeling og virkemåte:

- ✓ Ulikheter i organisering og virkemåte kan føre til at det oppstår gap og uklare grensesnitt hvor enkelte virksomheter ikke dekkes tydelig av SRM.
- ✓ Det er ulike tolkninger av hvorvidt føringer i rammeverket for håndtering av IKT-sikkerhetshendelser er veiledende eller krav.
- ✓ Det er enkelte uklarheter knyttet til, og et ønske om å tydeliggjøre, rolle- og ansvarsfordelingen opp mot NSM, særlig knyttet til håndtering av hendelser.
- ✓ Rammeverket forutsetter at virksomhetene selv følger opp pålagt ansvar, herunder grunnsikring, men det er stor variasjon i hvorvidt virksomhetene har den nødvendige kompetansen og kapasiteten til det.

I det følgende gås det nærmere inn på utfordringer knyttet til hvert enkelt punkt.

3.1.1 Ulikheter i organisering og virkemåte

Det har i forbindelse med evalueringen blitt påpekt av flere SRM at responsmiljøene varierer betydelig når det gjelder organisering, kapasitet og virkeområde. Blant de SRM som KPMG har snakket med varierer antall ansatte mellom ett og over 20 årsverk. Variasjonen i antall årsverk reflekterer naturlig nok også responsmiljøenes oppgaveportefølje samt evne og kapasitet til å løse oppgavene. Det er store variasjoner også hva gjelder antall virksomheter som betjenes av det enkelte SRM. Enkelte SRM

har stort dekningsområde, med flere tusen virksomheter, mens andre kun betjener et lavt antall etater underlagt det overordnede departement eller direktorat.

Som det fremkommer av Tabell 2 er det også store variasjoner knyttet til hvordan dekningsområdet i praksis avgjøres. For de fleste SRM er dekningsområdet definert formelt via føringer gitt av overordnet departement. For enkelte SRM som blir finansiert gjennom medlemsavgifter, blir dekningsområdet definert i praksis av hvorvidt virksomheter selv velger å inngå medlemskap og få tilknytning til responsmiljøene og tjenestene som tilbys.

De ulike SRM har også ulik tjenesteportefølje. Eksempelvis har noen en koordinerende rolle, mens andre har en operativ rolle i hendelseshåndtering eller bistår virksomhetene med teknisk IKT-drift. De fleste SRM som KPMG har gjennomført samtaler med oppfatter ikke at deteksjon og operativ hendelseshåndtering i utstrakt grad skal være en del av deres tjenester. Imidlertid er det eksempler på SRM som definerer hendelseshåndtering som en tjeneste de skal yte til sine medlemmer.

Tjenestetilbudet er i enkelte tilfeller påvirket av finansieringsmodellen, når virksomhetene selv kan velge om de inngår medlemskap med SRM eller ikke, og dermed får tilgang til ulike tjenester.

Store variasjoner i organisering og virkemåte har blitt trukket frem som en utfordring av flere SRM, samt av andre aktører på overordnet nivå, NSM inkludert. Det uttrykkes blant annet at dette fører med seg usikkerhet rundt hvorvidt hele sektorer er dekket eller ikke, og hvilke tjenester som tilbys. I disse tilfellene er det vanskelig for NSM å vite om hele sektoren blir varslet, eller hvilke deler av sektoren ikke er dekket av varslingen via SRM, og dermed ikke inkludert i systematisk varsling fra NSM via SRM til virksomhetene. Det oppleves også av flere SRM at det i liten grad er gitt klare føringer og forventninger til hensiktsmessig organisering.

3.1.2 Ulike tolkninger av føringer i Rammeverk for håndtering av IKT-sikkerhetshendelser

De sektorvise responsmiljøene er tillagt flere ulike ansvarsområder i den nasjonale modellen for håndtering av IKT-sikkerhetshendelser, herunder et særskilt ansvar for å holde oversikt over egen sektor, være informasjonsknutepunkt for alle relevante virksomheter, samt være sektorens bindeledd mot nasjonal responsfunksjon. NSM er etter sikkerhetsloven § 9 tillagt det nasjonale ansvaret for å koordinere håndtering av alvorlige IKT-sikkerhetshendelser mot kritisk infrastruktur. Selv om ansvaret for håndtering av IKT-sikkerhetshendelser er fordelt og lagt til flere aktører på ulike nivå, følger det av ansvarsprinsippet at virksomhetene selv har et særskilt ansvar for å håndtere IKT-sikkerhet i egen virksomhet.

Til tross for at det legges en rekke føringer for SRMs ansvarsområder i rammeverket, foreligger det ingen rettslig plikt for sektorer til å implementere krav og tiltak i rammeverket. Flere har i intervjuer uttrykt at det er delvis uklart hvorvidt føringene som er gitt i rammeverket er veiledende eller fastsatte krav, og ikke alle krav oppleves like relevante. Dette, i kombinasjon med at SRM har store variasjoner i organisering, størrelse og medlemsmasse har ledet til at ulike SRM har tilnærmet seg sitt ansvar ulikt. Det er blant annet store variasjoner i hvilke kjerneoppgaver og tjenester de tilbyr overfor sine underlagte virksomheter.

Videre oppleves det at man ikke i tilstrekkelig grad tolker nasjonale føringer likt, samt at overordnet departement har ulike tilnærminger og behov for ivaretakelse av egen sektor.

3.1.3 Ansvars- og oppgavefordeling mellom SRM og NSM

Den nasjonale modellen for håndtering av IKT-sikkerhetshendelser involverer et mangfold av aktører på ulike nivåer i det norske forvaltningssystemet. I Rammeverk for håndtering av IKT-sikkerhetshendelser er ansvar og grensesnitt beskrevet for en rekke av disse rollene, og spesielt for de tre nivåene rammeverket bygger på; virksomhet/systemeier, SRM og NSM.

Selv om både SRM og NSM opplever at samarbeidet fungerer godt, er det identifisert enkelte utfordringer knyttet til ansvars- og oppgavefordeling mellom dem. Flere opplever at rammeverket ikke

er tydelig nok i beskrivelsen av rollene og oppgavene, eller hvilken informasjon som deles med hvilken aktør, hvilket skaper uforutsigbarhet. De største uklarhetene gjelder forventningene til hendelseshåndtering; i hvilken grad kan SRM forvente å få bistand av NSM i en hendelse og hvordan vil ulike hendelser bli prioritert. Det påpekes at det er liten grad av transparens knyttet til NSMs prioriteringer, hvilket skaper usikkerhet rundt hva SRM kan forvente av NSM ved parallelle hendelser.

Klart definerte ansvarsforhold er viktig for å tydeliggjøre forventninger mellom partene. Til tross for at NSM i rammeverket ikke forventes å bistå med analysekapasitet i hendelseshåndtering, er dette kapasiteter NSM besitter og kan bistå med ved behov. At NSM ved enkelte anledninger yter flere tjenester enn hva som presenteres i rammeverket synes å skape en viss usikkerhet knyttet til hva SRM kan forvente av NSM, og den reelle leveranseevnen innen ulike analysedisipliner. Dette kan føre til en (potensielt feilaktig) oppfattelse av at egen sektor ikke prioriteres.

At dagens SRM har såpass ulik størrelse og modenhet skaper utfordringer for NSM. Ettersom NSM i dag i stor grad utveksler den samme informasjonen til alle SRM blir det utfordrende å finne riktig nivå på informasjonen som deles. Noe informasjon vil eksempelvis bli for avansert for de minst modne SRM, som i større grad ønsker seg informasjon og rådgivning knyttet til etablering av kapasiteter. Det er utfordrende for NSM å vite hvilke forventninger de kan ha til SRM, og hvilken rolle SRM forventer at NSM har overfor dem.

3.1.4 Ansvars- og oppgavefordeling mellom SRM og virksomheter

Rammeverket tar utgangspunkt i at virksomhetene selv har implementert god grunnsikring og har kompetanse innen deteksjon, vurdering og håndtering av hendelser samt at de varsler SRM. Det fremstår derimot for flere SRM som at virksomhetene selv har varierende grad av kjennskap til sitt ansvar, samt mulighet til å ivareta dette som følge av blant annet manglende kompetanse og kapasitet. Følgelig opplever en del SRM å bruke mye tid på å bistå med oppgaver som virksomhetene skal ivareta selv. Flere SRM opplever det som uklart hvor operativt SRM skal bistå virksomhetene, og hva som er den beste måten å støtte virksomhetene på. Enkelte har bevisst valgt å ikke tilby tjenester som kan leveres av private aktører. Flere ser behovet for å gjøre mer enn å oppdage og varsle hendelser, herunder å bistå med mer forebyggende arbeid. NSMs grunnprinsipper nevnes i flere samtaler som et godt verktøy for å støtte virksomhetene med grunnsikring.

Det nevnes også en viss bekymring for at de større medlemmer får litt mindre nytte av ordningen, siden de har omfattende kapasitet og kompetanse selv. Samtidig finnes det tilfeller hvor man utnytter samarbeidet med de store virksomhetene bedre, og virksomhetene ser verdien av å bidra til økt sikkerhet i sektoren.

3.1.5 Formalisering og tilknytning til overordnet departement

Det er variasjoner i SRMs tilknytning til overordnet departement. Noen SRM er tydelig utpekt av overordnet departement og har en klart definert sektor som sitt dekningsområde. Andre er ikke direkte utpekt som SRM av sitt overordnede departement, men har inngått en avtale med aktører som er utpekt SRM slik at disse to til sammen ivaretar SRM-funksjonen for sin sektor. Det er viktig å påpeke at dette nødvendigvis ikke oppleves som en utfordring. Samtidig kan en slik rollefordeling fordre ekstra avklaringer vedrørende ansvarslinjer og grensesnitt mellom de involverte aktørene.

Intervjuene gir et overordnet inntrykk av at SRM opplever varierende klarhet i føringer fra overordnet departement. Enkelte har relativt stor grad av frihet til å utføre sine oppgaver, med lite kontroll fra overordnet departement. Enkelte ønsker i denne sammenhengen mer strategisk styring og dialog. Samtidig oppgir andre å ha klare instrukser og føringer om hvilke oppgaver som skal legges til SRM, spesielt de SRM som har et aktivt styre med representanter med bakgrunn fra informasjonssikkerhet.

3.1.6 Forholdet mellom en myndighet og et utpekt som ikke er en del av myndigheten

Det er noe variasjon i dag om SRM er en del av myndigheten eller ikke. Fra evalueringen fremstår dette ikke som en særskilt utfordring. SRM som ikke er en del av myndigheten har ofte avtalefestet hvilke oppgaver de skal løse i kontrakt med den myndigheten som er formelt utpekt som SRM. Så lenge slike avtaler er på plass fremstår det ikke som problematisk at SRM ikke er direkte underlagt myndigheten. Det er eksempler på at ekstra oppgaver som departementet pålegger SRM knyttet til eksempelvis varsling av virksomheter som ikke er medlemmer, er finansiert via statsbudsjettet.

3.2 Utfordringer vedrørende sektorprinsippet

Gjennom intervjuer er det blitt identifisert enkelte utfordringer knyttet til sektorprinsippet. Flere peker på et gap mellom cybersikkerhetsområdets sektorovergripende natur og sektorprinsippet i staten. Det oppleves videre at sektorbegrepet ikke er tydelig nok definert i rammeverket eller i den nasjonale strategien for digital sikkerhet. Det er også stor variasjon i hvordan en sektor er definert som dekningsområde for SRM; for enkelte er det kun direkte underliggende etater, mens andre har en bredere definisjon som også inkluderer private virksomheter.

Begrepet «sektorvist responsmiljø» kan derfor føre med seg en viss grad av falsk trygghet, all den tid dekningsområdet varierer så mye som den gjør i dagens situasjon. På papiret er det utpekt og etablert et SRM som pålagt i rammeverket, men i realiteten er det uklart om hele sektoren er ivaretatt og for eksempel blir varslet gjennom SRM.

Enkelte departement har brede ansvarsområder, og opplever at det er problematisk å samle dette under en og samme sektorbetegnelse med et utpekt SRM. I disse tilfellene vurderer departementet å etablere flere SRM. Fra NSM sitt ståsted er det en utfordring om flere departement har flere «undersektorer» med respektive SRM, da dette vil øke antall SRM betydelig. Det oppleves også at rammeverket ikke passer inn i tverrsektorielle samarbeid, da det er uklart hvilket departement som i så fall er ansvarlig for SRM.

Det oppleves utfordrende å implementere rammeverket på en måte som inkluderer det private næringslivet i dekningsområdet. Virksomheter kan være del av flere sektorer, hvilket gjør det krevende å avgjøre et tilhørende SRM. Når departementet kan styre de underlagte virksomhetene direkte, er rammeverket relativt enkelt å gjennomføre. Når private aktører er inkludert i dekningsområdet, oppleves det at departementet ikke kan pålegge private aktører oppgaver, men må basere seg på frivillighet.

Enkelte departement har vurdert at de økonomiske rammene begrenser muligheten til å etablere SRM, samt at det finnes få samfunnskritiske funksjoner i sektoren. I noen tilfellene har departement avtalt samarbeid med en annen sektor for de relevante virksomhetene, eller har en mindre enhet som formidler varsling mellom virksomhetene og NSM. Enkelte har etablert samarbeid direkte mellom operative miljøer og NSM og ser ikke merverdi i å etablere SRM.

Flere departement fremhever spesielle behov i sin sektor som en av grunnene til å utpeke et eller flere SRM i egen sektor. Etter KPMGs erfaring er behovene knyttet til forebyggende og operativ IKT-sikkerhet ofte sammenfallende som gjør det hensiktsmessig å vurdere felles løsninger så langt det lar seg gjøre.[3]

Sektorprinsippets effekt for håndtering av og forberedelse til akutte kritiske hendelser har vært kritisert og diskutert både før og etter kriser i samfunnet. Utfordringene er gjentakende og henger nært sammen med at det ikke er en enkelt person som sitter med det fullstendige ansvaret for beredskapen og håndteringen av konkrete hendelser. Sektorprinsippet er først og fremst utfordrende i

[3] Relevant rapport i denne sammenheng: ENISA Report - Sectoral CSIRT capabilities - Energy & Air Transport.pdf

den grad det fører til sektoriell tankegang blant aktørene i de forskjellige sektorene og på den måten hindrer samhandling og effektiv planlegging for håndtering av akutte hendelser. Effektiv krisehåndtering krever samhandling på tvers av etater og tverrsektoriell koordinering[4]. For å minimere utfordringene som følger av sektorprinsippet er det vesentlig å kunne gjennomføre øvelser og annen type samhandling på tvers av sektorene før en kritisk hendelse finner sted. Et av de viktigste premissene for å kunne håndtere tverrsektorielle hendelser av ukjent natur er at sektorene finner sammen og kjenner til hverandres kapasitet og handleevne. På den måten vil en bryte ned de utfordringene sektorprinsippet skaper og heller dra nytte av sektoriell spisskompetanse i hvert enkelt tilfelle – hvilket er begrunnelsen for sektorprinsippet i seg selv.

3.3 Kompetanse og kapasitet

En felles utfordring for alle aktører i ordningen er at det er krevende å tiltrekke seg, og å beholde, relevant digital sikkerhetskompetanse. Etterspørselen etter slik kompetanse har økt kraftig de siste årene. Stadig flere tjenester flyttes over i det digitale domenet, og digitale trusler har blitt noe alle virksomheter må forholde seg til. Dette betyr at det er høy etterspørsel etter et begrenset antall ressurser. Mange SRM rapporterer om at det er vanskelig å beholde kompetanse i organisasjonen. NSM samt SRM innen offentlig sektor med tilhørende lønnsnivå kan komme til kort i rekrutteringsprosessen, fordi privatmarkedet kan tilby mer gunstige betingelser. Når de klarer å tiltrekke seg nyutdannede, er det ikke uvanlig at disse beveger seg videre til privatmarkedet etter noen år, når de har opparbeidet seg erfaring. Dette gjør at det brukes mye tid på opplæring av ressurser som beveger seg videre etter relativt kort tid.

Størrelsen på organisasjonen oppleves som en mulig faktor i å tiltrekke og beholde kompetanse. Det å være et større fagmiljø med høy modenhet synes å være et konkurransefortrinn hva gjelder å tiltrekke og beholde relevant kompetanse. Dette kan være knyttet til at miljøene oppleves som mer interessante for potensielle arbeidstagere – for eksempel vil de ha mer kapasitet til å utøve opplæringsaktiviteter, og arbeidsoppgavene vil i noen tilfeller være mer varierte.

Dagens modell legger opp til at alle departementer skal utnevne et responsmiljø for sin sektor. Dette innebærer at kompetanse plasseres mange ulike steder, og til dels i funksjoner der det reelle ressursbehovet er lavt. Modellen legger med andre ord opp til at kompetanse «smøres tynt utover» de ulike sektorene. Dette er en utfordring, fordi det kan føre til ineffektiv ressursbruk i en bransje med stor konkurranse om kompetanse.

3.4 Private aktørers rolle

Den nasjonale motstandsdyktigheten mot digitale angrep er i stor grad avhengig av IKT-infrastruktur som eies av private aktører. Dette inkluderer internasjonale leverandører som Google, Microsoft og Amazon, samt norske aktører som Telenor og Telia.

I dagens Rammeverk for håndtering av IKT-sikkerhetshendelser fremkommer det ikke hvilken rolle private leverandører av IKT-infrastruktur og andre samfunnsviktige tjenester skal ha i den overordnede modellen. Det samme gjelder for leverandører av sikkerhetstjenester knyttet til deteksjon og hendelseshåndtering, som eksempelvis de godkjente aktørene innen hendelseshåndtering i NSMs kvalitetsordning.

Inkludering av private aktører i SRM-forum i dag synes å bære preg av en organisk vekst av forumet. Noen SRM opplever at flere private aktører burde vært inne i SRM-forumet, andre mener at private aktører ikke burde opptre i SRM-forumet. Det er enighet i at samarbeid med private aktører er viktig for den nasjonale motstandsdyktigheten, men at det er en utfordring at kun enkelte private aktører har

[4] Boin, A., 'T Hart, P. (2007). The Crisis Approach. I: Handbook of Disaster Research. Handbooks of Sociology and Social Research. Springer, New York, NY. https://doi.org/10.1007/978-0-387-32353-4_3

tilgang, uten at begrunnelsen for det er tydelig. Det fører blant annet med seg kommersielle utfordringer, ved at det oppleves at private aktører kan få et konkurransefortrinn gjennom slik tilstedeværelse, og dette igjen kan forhindre effektivt samarbeid og informasjonsdeling i SRM-forumet.

Både NSM og SRM ser behov for et tett samarbeid med private aktører og ønsker en klargjøring av private aktørers rolle i rammeverket for håndtering av IKT-sikkerhetshendelser. eksempelvis i form av klare retningslinjer og kriteria for hvem som skal og ikke skal ha en rolle i den nasjonale ordningen for hendelseshåndtering.

3.5 Kommunikasjon og samarbeid

God kommunikasjon og godt samarbeid er en grunnleggende forutsetning for å skape god situasjonsoversikt og for å effektivt kunne håndtere og redusere konsekvensene av alvorlige IKT-sikkerhetshendelser. Kommunikasjon handler om å formidle og dele informasjon rettidig og ved hjelp av egnede kommunikasjonskanaler. Effektiv utveksling av informasjon innebærer ikke bare overføring av relevant informasjon til mottakeren – like viktig er det at mottakeren får god forståelse av situasjonen og har tilstrekkelig kompetanse til å forstå det som kommuniseres.

Rammeverket beskriver en rekke forventninger til virksomheter, SRM og NSM når det kommer til hvordan de ulike aktørene i ordningen skal samarbeide for å skape god situasjonsoversikt og for å best mulig utnytte samfunnets samlede ressurser for å effektivt håndtere hendelser. Prosedyrer for koordinering, rapportering og ansvarsdeling er med på å definere samarbeidsklimaet og legge til rette for effektive prosesser på tvers av organisatoriske enheter. SRM forventes blant annet å besitte en viss kunnskap om kritisk infrastruktur i egen sektor og virksomheter skal delta i samhandlingsøvelser.

Videre presenteres identifiserte utfordringer knyttet til kommunikasjon og samarbeid mellom NSM og SRM, mellom SRM og til slutt mellom SRM og virksomheter.

3.5.1 Samarbeid mellom NSM og SRM

NSM er det nasjonale fagmiljøet for IKT-sikkerhet og har en nøkkelrolle i koordinering og distribusjon av sikkerhetsrelatert informasjon. Ettersom NSM også er tillagt det nasjonale ansvaret for å koordinere håndtering av alvorlige IKT-sikkerhetshendelser er samarbeid en svært viktig del av NSMs virke. Det har fremkommet gjennom våre intervjuer at det utføres mye godt arbeid fra NSM knyttet til samarbeid og informasjonsdeling, men enkelte forhold blir også utfordret og problematisert.

Flere SRM trekker frem viktigheten av å bygge relasjoner på tvers av SRM og NSM. Det bemerkes av enkelte SRM at tillitt er ekstra viktig for personell som jobber med sikkerhet og at strukturer og prosedyrer i liten grad kan erstatte mellommenneskelig tillitt og relasjoner. Gode relasjoner kan skape effektivt samarbeid. Samtidig er det problematisk dersom samarbeidet i for stor grad beror på mellommenneskelige relasjoner i et arbeidsmarked med stor turnover.

NSM legger til rette for samarbeid med SRM ved hjelp av flere ulike fora og kanaler, blant annet Teams, IRC, Mattermost, og e-post. Blant SRM er det noe misnøye knyttet til de tekniske løsningene som skal understøtte samarbeidet med NSM. Et høyt antall kanaler og verktøy blir trukket frem som en utfordring både av SRM og NSM.

SRM er ikke underlagt sikkerhetsloven, og ikke klarert for skjermingsverdig informasjon og har således ikke tilgang til gradert samhandling. Dette opplever alle parter - NSM, SRM og departementene - som en utfordring som forsinker og forhindrer informasjonsdeling, spesielt i nasjonale kriser.

3.5.2 Samarbeid mellom SRM

I dagens modell legges det også opp til samarbeid mellom SRM. Det forventes blant annet at SRM skal varsle om IKT-sikkerhetshendelser til andre SRM, og på den måten skape effektiv informasjonsflyt om relevante hendelser på tvers av sektorer.

NSM legger til rette for samarbeid mellom SRM. For å sikre bred informasjonsdeling har NSM etablert flere fora for informasjonsdeling fra NSM til SRM. I disse foraene blir det også oppfordret til deling av informasjon fra SRM slik at kunnskap og erfaringer flyter på tvers. Eksempelvis gjennomføres det virtuelle koordineringsmøter annenhver uke og fysiske SRM-møter kvartalsvis. Under disse møtene oppfordres SRM til å dele informasjon om hendelser innen sitt respektive dekningsområde slik at NSM får oppdatert situasjonsforståelse både sektorvis og tverrsektorielt.

En fundamental forutsetning for informasjonsdeling er tillit blant SRM. Også blant SRM er tillit i stor grad basert på at deltakere kjenner hverandre, har jobbet sammen over en lengre periode og kjenner hverandres kompetansenivå. En utfordrende faktor i dagens situasjon er det økende antallet deltakere i samarbeidsforaene. Ettersom stadig flere SRM etableres, blir det flere deltakere i foraene, og det oppleves som mindre oversiktlig.. Dette fører til tilbakeholdenhet knyttet til informasjonsdeling. Når i tillegg modenheten i SRM varierer, svekkes tilliten til at alle i SRM-ordningen evner å håndtere informasjonen i henhold til behovet for skjerming. Mindre modne SRM kan også ha høyere terskel til å dele informasjon eller delta diskusjonen i ulike fora. Dette medfører at det formes mindre grupper av SRM som jobber tettere med hverandre.

Tillit kan også fasiliteres ved hjelp av felles struktur og retningslinjer. Trafikklysprotokollen[5] (TLP) blir trukket frem som et eksempel i denne kontekst. Flere SRM benytter TLP ved deling av informasjon til andre SRM. Samtidig er enkelte SRM usikre på hvorvidt alle SRM forstår hvordan informasjon skal håndteres i henhold til TLP og de velger derfor å sende med en beskrivelse av TLP-definisjonen når informasjonen merkes med TLP. I tillegg er det noen juridiske utfordringer i bruk av TLP, spesielt med TLP:RØD når en enkelt ansatt har informasjon som kan ramme virksomheten, men ikke er tillatt av protokollen å dele informasjon videre inn i organisasjonen.

Det synes å være ganske store forskjeller på hvor mye de ulike SRM deler i de etablerte samarbeidsforaene. Enkelte SRM er veldige aktive og deler mye. På den andre siden er det flere SRM som i all hovedsak mottar informasjonen uten å selv dele, hvilket påvirker villigheten til å dele og tilliten hos andre SRM. Konkret blir det vist til at det for enkelte SRM er ønskelig med mer avgrensede fora for å fremme delingsvilje. Det råder en oppfatning blant en del SRM om at spennet mellom de SRM er i ferd med å bli såpass stort at verdien av å samhandle på tvers avtar.

For å formalisere samarbeidet mellom SRM, etterlyses det en formell samarbeidsavtale. Dette er en forutsetning for effektivt samarbeid ved en hendelse for å kunne dele eksempelvis ressurser, kompetanse og informasjon logger som kan inneholde personopplysninger. Enkelte SRM trekker også frem et behov for felles øvelser.

3.5.3 Samarbeid mellom SRM og virksomheter

Hvordan SRM samarbeider med virksomhetene i deres sektor varierer avhengig av SRMs størrelse, tjenesteportefølje og modenhet, i tillegg til sektorens generelle modenhet innen IKT-sikkerhet. Generelt sett synes det å være en sammenheng mellom sektorens generelle modenhet innen IKT-sikkerhet og SRMs modenhet. Sektorer som over tid har vært særlig utsatt for digitale trusler har også over tid hatt behov for å utvikle kapasiteter, og således kommet lenger når det kommer til samhandling og informasjonsdeling.

De mest modne SRM har på bakgrunn av sin kompetanse og tjenesteportefølje bedre forutsetninger for å rådgi virksomhetene i sin sektor. Et SRM kan kjenne godt til trussel- og sårbarhetsbildet i egen sektor ved å kun være en informasjonsknutepunkt for denne type informasjon. Likevel vil SRM som også utfører deteksjon og/eller sårbarhetshåndtering gjerne besitte en dypere kunnskap om aktuelle

[5] Traffic Light Protocol (TLP) (first.org)

trusler og sårbarheter, og på bakgrunn av denne kunnskapen være bedre rustet for å gi konkrete råd om hvordan virksomhetene i sektoren skal kunne sikre seg og oppdage relevante trusler, eller hvilke tiltak som bør iverksettes for å utbedre sårbarheter.

Det er stor variasjon i IKT-sikkerheten i norske virksomheter. Disse variasjonene gir utslag på virksomhetenes opplevde behov for SRM-ordningen. Virksomhetene som over tid har opparbeidet seg høy modenhet innen operativ IKT-sikkerhet synes i mindre grad å se verdien av SRM, da de selv mottar trusselinformasjon gjennom egne kilder noen ganger til og med raskere enn hva som deles fra SRM og samtidig har etablert samarbeid med andre modne virksomheter. Til tross for at de modne virksomhetene har mindre bruk for SRM, så har de mest å bidra med inn i SRM-ordningen og generelt sett synes det å være slik at det er de mest modne virksomhetene som samarbeider tettest opp mot sitt SRM.

I andre enden har man virksomheter med lav modenhet innen IKT-sikkerhet. For at virksomhetene skal kunne få verdi av trussel- og sårbarhetsvarsler fra et SRM må virksomheten ha en viss kompetanse og kapasitet til å motta, behandle og agere på informasjonen som kommer fra SRM. Uten tilstrekkelig kapasitet vil varslene gi liten verdi for virksomhetene som mottar disse. Virksomhetene med lav modenhet er således også de virksomhetene som jobber minst opp mot sitt SRM. Enkelte ønsker derfor at NSM skal kunne pålegge virksomhetene et grunnleggende sikkerhetsnivå.

Hvor mye rådgivning SRM gir til virksomhetene i sin sektor varierer, og det samme gjør virksomhetenes ønske om råd og veiledning fra SRM. Slike tjenester har enkelte SRM avtaleregulert for å skape tydelighet i SRMs leveranser. Flere SRM ønsker å skille mellom tjenester som SRM kan levere sammenlignet med tjenester som private virksomheter tilbyr for å unngå å konkurrere med private virksomheter, mens andre har tjenester som kan sammenlignes med drift- eller rådgivningstjenester innen IT og informasjonssikkerhet.

3.6 Oppsummerende vurderinger og anbefalte prinsipper for videreutvikling

Dette kapittelet introduserer noen overordnede prinsipper for den videre utviklingen av ordningen. Formålet med prinsippene er å bidra til styrking av den nasjonal evnen til å avdekke og håndtere digitale angrep gjennom å fokusere ressurser til de sektorene som har virksomheter med betydning for grunnleggende nasjonale funksjoner, men samtidig sørge for en grunnleggende dekning i alle sektorer.

Hvert prinsipp hviler på vurderinger av utfordringsbildet som er presentert i delkapitlene overfor. Kapittel 4 presenterer en alternativ modell for ordningen med SRM som bygger på prinsippene. KPMG mener, uavhengig av endelig valgt organisering og retning for ordningen, at prinsippene under bør legges til grunn for å møte utfordringene og behovene som har blitt identifisert i denne evalueringen.

Følgende prinsipper foreslås for videreutvikling av ordningen med SRM:

Prinsipp 1: Rammeverket bør i større grad inkludere forebyggende arbeid med IKT-sikkerhet i tillegg til operative aktiviteter innen hendelseshåndtering

For å redusere konsekvensene og raskest mulig gjenopprette normaltilstand ved en hendelse er det nødvendig å håndtere den effektivt etter en definert prosess. Hendelseshåndtering er en prosess som

kan beskrives med følgende faser; forberedelse; deteksjon og analyse; skadebegrensning og gjenoppretting; og evaluering og læring. Når hendelsen inntreffer er det for sent å utarbeide planverk, prosedyrer, rapporteringsrutiner og kommunikasjonsstrategier. Derfor inngår forberedelse som en sentral del av selve prosessen. Selv om dagens rammeverk beskriver sentrale aspekter og forventninger til aktørene innen håndtering av IKT-sikkerhetshendelser, mangler både tydeliggjøring og oppfølging av oppgavene. Metoden for å klassifisere IKT-sikkerhetshendelser fremstår lite hensiktsmessig og vil gi lite verdi ved en reell hendelseshåndtering.

Rammeverket for håndtering av IKT-sikkerhetshendelser dekker i liten grad de forebyggende aktivitetene som bør gjennomføres av en operativ IKT-sikkerhetsfunksjon, utover ren hendelseshåndtering. Anerkjente rammeverk for operative IKT-sikkerhetsfunksjoner belyser viktigheten av å levere flere ulike tjenestekategorier. FIRST sitt rammeverk (se Vedlegg 1 for mer informasjon om rammeverket), benytter tjenestekategoriene deteksjon, hendelseshåndtering, sårbarhetshåndtering, situasjonsforståelse og kunnskapsdeling. Disse tjenestekategoriene gjenspeiler viktigheten av koblingen mellom det forebyggende og det operative arbeidet som gjøres av operative IKT-sikkerhetsfunksjoner.

Erfaring viser at operative IKT-sikkerhetsfunksjoner bør ha en helhetlig tilnærming og utnytte synergier av å etablere kapabiliteter som understøtter hverandre. Det bør være klare koblinger mellom utførelse av operativt arbeid innen deteksjon og hendelseshåndtering og videreutvikling av egne operative kapabiliteter. På samme måte bør arbeid med trussel- og sårbarhetsinformasjon benyttes for å styrke motstandsdyktigheten mot angrep og evnen til å avdekke og håndtere digitale angrep.

En ny eller revidert modell bør i større grad inkludere forebyggende arbeid innen IKT-sikkerhet og balansere dette mot det operative arbeidet som utøves. Samtidig bør forventninger til partene innen de ulike tjenestekategoriene tydeliggjøres og følges opp. Det vil også være hensiktsmessig å videreutvikle rammeverkets klassifisering av IKT-sikkerhetshendelser. Klassifiseringen kan forenkles til konkrete nivåer og til å inkludere hvem som er ansvarlig eller bør være involvert innenfor de ulike nivåene, samt hva de ansvarlige bør gjøre[6].

Prinsipp 2: Den nasjonale innsatsen bør kraftsamles for å sikre grunnleggende nasjonale funksjoner

Sektorprinsippet som ligger til grunn for dagens ordning har den begrensning at digitale sikkerhetshendelser svært ofte rammer på tvers av sektorielle skillelinjer. Samhandlingen mellom SRM, som i hovedsak foregår i SRM-forumet, fungerer som et organ der erfaringer og innsikt kan deles og diskuteres.

Det vil være hensiktsmessig å danne samarbeidsstrukturer som i større grad er fokusert mot koordinert innsats mot felles mål, der man jobber sammen både forebyggende og operativt. Det er ikke realistisk å få til slikt samarbeid rettet mot alle virksomheter – til det er antall virksomheter for stort. Det bør heller gjøres et utvalg av virksomheter som har avgjørende betydning for grunnleggende nasjonale funksjoner.

En slik samarbeidsstruktur vil kunne styrke den helhetlige motstandsevnen mot digitale angrep rettet mot samfunnets viktigste funksjoner. Det vil i mindre grad være bundet av sektorprinsippet, men heller være fokusert mot grunnleggende nasjonale funksjoner, uavhengig av sektortilhørighet. Offentlige og private virksomheter som har avgjørende betydning for grunnleggende nasjonale funksjoner bør inngå i en slik samarbeidsstruktur sammen med NSM og tilhørende SRM. Dette kan åpne for tettere samarbeid både forebyggende og operativt der det kan legges til rette for deling av gradert informasjon og der tillitsnivået er høyt. Man vil videre kunne basere seg på lovkrav gitt i sikkerhetsloven (ettersom disse virksomhetene vil være underlagt denne).

[6] NCSC-UK har utarbeidet et system for kategorisering av IKT-sikkerhetshendelser som kan benyttes som utgangspunkt eller inspirasjon: New Cyber Attack categorisation system to improve UK... - NCSC.GOV.UK

Prinsipp 3: Spesifikke sektorvise behov skal ligge til grunn for opprettelsen av SRM

SRM skal løse oppgaver som ikke kan løses på nasjonale nivå eller av virksomhetene selv. Dette innebærer at hvis det ikke avdekkes oppgaver som mest hensiktsmessig kan løses på sektornivå, bør man ikke opprette SRM. For de sektorene der det er vurdert hensiktsmessig med et SRM, men man ikke alene har nok kapasitet eller kompetanse til å ivareta minimumskravene kan det være et alternativ å søke samarbeid med andre SRM som kan dekke mer enn en sektor. Slik kan man bedre utnytte ressursene og sikre sterkere miljøer.

Det bør også vurderes om en felles-funksjon bør løftes til nasjonalt nivå og ligge under NSM. En sånn fellesfunksjon kan dekke alle virksomheter som ikke har naturlig tilknytning til sektor eller i en sektor uten SRM.

En viktig forutsetning for god informasjonsdeling, sparring og samhandling mellom miljøene er at det er høy tillit mellom samarbeidspartene. Flere peker på at en av suksessfaktorene med dagens ordning er at det størrelsesmessig er en oversiktlig gruppe med høy tillit og stor delingsvilje. I et scenario med et stadig økende antall SRM og et samarbeidsforum som vokser i størrelse, risikerer man redusert oversikt og tillitspulverisering. Det fremstår derfor lite hensiktsmessig å komme i en situasjon der antall SRM blir uhåndterlig høyt.

Prinsipp 4: Det bør etableres formelle minimumskrav for et utpekt SRM

Basert på utfordringsbildet er det flere forhold som taler for at man bør etablere formelle minimumskrav for SRM. Først og fremst vil det trolig lede til større grad av tydelighet overfor NSM og andre SRM, andre sentrale aktører i ordningen og sektoren de representerer. Dette kan igjen redusere eventuelle forventningsgap og tydeliggjøre rollen de har overfor virksomhetene i sektoren og øvrige nøkkelaktører.

Som det fremkommer av utfordringsbildet er det også variasjoner i hvordan ulike SRM har tilnærmet seg og tolket føringer i rammeverket for håndtering av IKT-sikkerhetshendelser. Det er i svært varierende grad 1) operasjonalisert og 2) implementert som integrert, styrende dokument. Minimumskrav knyttet til for eksempel noen nøkkelfunksjoner og dekningsgrad i sektoren vil etter vår vurdering gi tydelighet rundt hva som faktisk skal dekkes av et SRM, både overfor virksomhetene i sektoren, de øvrige SRM og for NSM.

Et sett med minimumskrav vil sikre at et miljø må oppfylle en viss funksjon i tråd med ordningens formål før det får status som sektorvis responsmiljø. SRM bør fortsatt stå fritt til å utvide tjenestetilbudet utover dette, i tråd med sektorens behov.

Det kan være hensiktsmessig å knytte minimumskravene til bredden av tjenestekategorier, herunder deteksjon, hendelseshåndtering, sårbarhetshåndtering, situasjonsforståelse og kunnskapsdeling (se prinsipp 1).

Minimumskravene som settes bør følges av tilstrekkelig finansiering for å innfri kravene i de tilfeller der SRM ikke er finansiert over statsbudsjettet.

Prinsipp 5: De ulike aktørenes rolle i hendelseshåndteringen bør nyanseres og tydeliggjøres

I rammeverket bør det fremkomme tydelig i hvilke tilfeller de ulike aktørene (NSM, SRM og virksomheter) skal bidra i hendelseshåndteringen, med hvilken kapasitet og på hvilken måte. Slik kan man redusere variasjonen av forventninger til de ulike aktørene og gi økt forutsigbarhet for samarbeidspartnere og virksomheter. Det vil også tydeliggjøre overfor virksomhetene hva de selv forventes å håndtere. En omforent modell for samhandling som inkluderer en tydelig beskrivelse av oppgaver og ansvar vil kunne bidra til tydeliggjøring av rollene.

Observasjoner gjennom arbeidet med denne rapporten har vist at private aktørers rolle, enten som SRM eller annen part involvert i IKT-hendelser varierer, og i liten grad er formalisert. Det foreligger ikke en avtalemodell som formaliserer samarbeidet mellom de ulike SMR og øvrige parter. Hvilken rolle private aktører skal ha i de ulike samarbeidsstrukturene bør formaliseres og inkluderingen av disse bør baseres på noen fastsatte kriterier. Dette bør være basert på GNF-prosessen og i hvilken grad en virksomhet er av vesentlig eller avgjørende betydning. For aktører som leverer sikkerhetstjenester innen områdene deteksjon og hendelseshåndtering bør deltagelse knyttes til om de leverer sikkerhetstjenester til virksomheter som er avgjørende for grunnleggende nasjonale funksjoner.

4 Videreutvikling av ordningen med SRM

Kapittel 4.1. beskriver KPMGs forslag til videreutvikling av ordningen med sektorvise responsmiljøer.

Kapittel 4.2. vurderer de administrative og økonomiske konsekvensene av foreslått modell (alternativ 1). For å vurdere de administrative konsekvensene har det også blitt gjennomført tilsvarende vurderinger for to andre alternativer:

- ✓ Alternativ 0 (fortsette som i dag, fortsatt mangelfull implementering av rammeverket for håndtering av IKT-sikkerhetshendelser)
- ✓ Alternativ 0+ (implementere føringer i Rammeverk for håndtering av IKT-sikkerhetshendelser, herunder at departementene utpeker SRM i de sektorene der det ikke er SRM per i dag)

Modellene med tilhørende antatte administrative og økonomiske konsekvenser er nærmere beskrevet i kapittel 4.2.

4.1 Forslag til videreutvikling av ordningen med SRM

Formålet med forslagene til videreutvikling av dagens ordning med sektorvise responsmiljøer er å nyansere ordningen og gjøre den mer behovstilpasset. Dette innebærer å bevege seg fra at det stilles like krav til alle sektorer og SRM, til å tillate ulike løsninger basert på om det er behov for en sektorspesifikk funksjon.

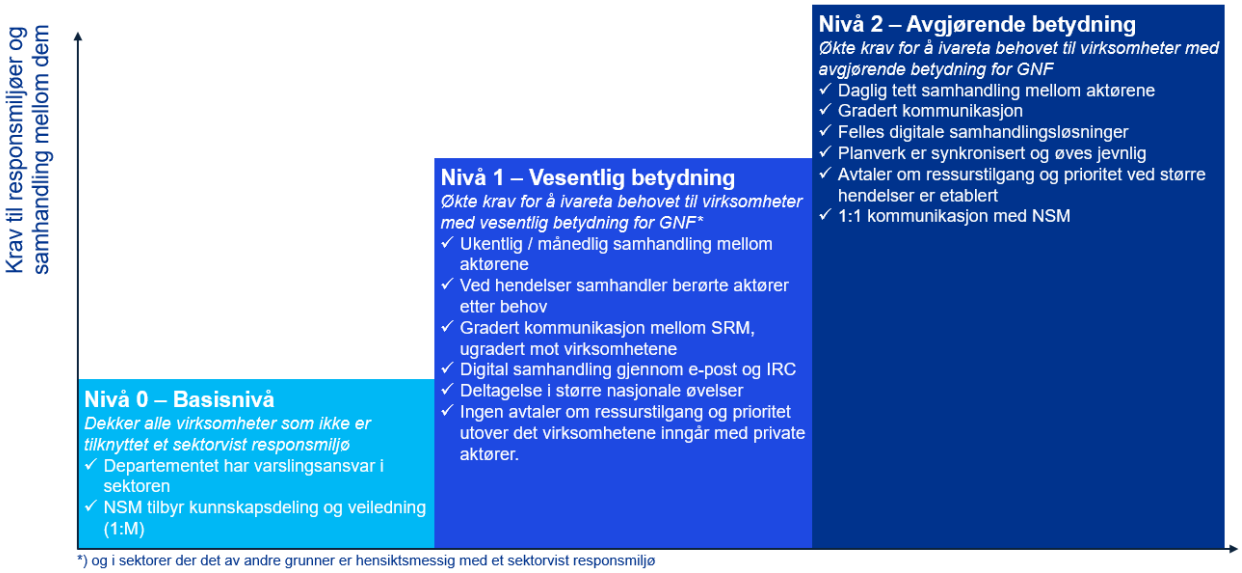
Det anbefales å stille ulike nivå av krav til responsmiljøene og samhandlingen mellom dem og sikkerhetsmyndigheten basert på følgende:

- ✓ hvor kritisk tilhørende virksomheter er for den nasjonale sikkerheten, og følgelig
- ✓ hvor omfattende konsekvenser en IKT-sikkerhetshendelse i disse virksomhetene vil få

Ettersom det pågår et arbeid i departementene med å identifisere grunnleggende nasjonale funksjoner og virksomheter som har vesentlig eller avgjørende betydning for disse, anbefales det å knytte nivåene i SRM-ordningen til dette arbeidet. Det foreslås en tre-nivå modell der samhandlingsnivået og minimumskravene øker med virksomhetenes betydning for grunnleggende nasjonale funksjoner. Det er viktig å påpeke at forslaget om minimumskrav utgjør et minimumsnivå, og at et SRM står fritt til å tilby ytterligere tjenester til sektoren der man vurderer dette som hensiktsmessig.

I tillegg anbefales det at det stilles noen basiskrav som gjelder uavhengig av tilknytning til SRM. Dette gjelder ivaretagelse av varsling i hele sektoren, samt generell kunnskapsdeling og tilgang til veiledere og kvalitetsordning for hendelseshåndtering fra NSM.

Figuren under illustrerer de tre ulike nivåene i forslaget til videreutvikling av modellen.



Figur 1 Anbefalt nivåinndeling for krav til responsmiljøer og samhandlingen mellom dem

Nivå 0 – Basisnivå

Formålet med basisnivået er å sikre at varsling innenfor alle sektorer blir ivaretatt, og at alle virksomheter har tilgang til generell kunnskapsdeling i form av veiledere og annen generell rådgivning via NSM.

Dette nivået er et minimumsnivå som gjelder for alle sektorer, og bør dekke alle virksomheter uavhengig av tilknytning til sektorvist responsmiljø. Dette innebærer blant annet at departementene har varslingsansvar i hele sektoren og til NSM. For de sektorene der det ikke er opprettet et SRM må varslingsansvaret ivaretas av departementet (eller delegeres til en annen aktør). Generell kunnskapsdeling og veiledning som er relevant for virksomhetenes håndtering av IKT-sikkerhetshendelser bør tilbys fra NSM i en én-til-mange-modell (1:M).

Minimumskravet om å utgjøre et kontaktpunkt i sektoren er i tråd med tiltak 38 i nasjonal strategi for digital sikkerhet.[7]

For alle virksomheter som ikke har naturlig tilknytning til sektor eller er i en sektor uten SRM, bør det vurderes hvorvidt det er behov for å danne en fellesfunksjon, for eksempel i NSM, som skal ha som oppgave å bistå denne gruppen virksomheter med informasjonsdeling, sårbarhetsvurderinger og lignende.

Nivå 1 – Vesentlig betydning

Formålet med nivå 1 er å sikre sektorspesifikk kompetanse i forbyggende og operativ IKT-sikkerhet i sektorer med virksomheter som har vesentlig betydning for GNF eller av andre grunner har behov for sektorspesifikk kompetanse og koordinering.

For sektorer der det er vurdert hensiktsmessig, skal det utpekes et SRM av departementet. Disse skal oppfylle et sett med minimumskrav for dette nivået. For å sikre at SRM har nok kapasitet og kompetanse til å ivareta minimumskravene kan ulike departementer velge å samarbeide om en funksjon, spesielt i sektorer med begrenset rolle i samfunnskritiske funksjoner.

SRM har ansvar for samarbeid og koordinering innenfor sektoren og mot andre sektorer for å ivareta sektorspesifikke behov. Det kan være behov knyttet til for eksempel medisinsk teknisk utstyr innen helse eller 5G innen Ekom. SRM skal formidle sektorspesifikk informasjon til NSM, og berike generell

[7] «Som en minimumsløsning skal det etableres et kontaktpunkt i sektoren for alvorlige IKT-hendelser og prosedyrer for varsling internt i sektoren og opp mot NSM NorCERT. Utover dette må sektorene selv vurdere hva slags behov de har for å håndtere alvorlige IKT-hendelser og hvordan de eventuelt skal skalere opp sine responsmiljøer»

informasjon fra NSM til virksomhetene i sektoren. SRM ivaretar også behovet for koordinering, informasjonsdeling og samarbeid mellom virksomhetene i sektoren. SRM koordinerer og deler informasjon innenfor sektoren og er bindeledd til/fra NSM. De sørger for at sektoren er oppdatert og at NSM er oppdatert på sektorens situasjon.

SRM samarbeider med hverandre og NSM i SRM-forum fasilitert av NSM. Virksomhetene har tilgang til en-til-mange dialog med NSM gjennom sårbarhetsvarsling, generell situasjonsforståelse, veiledere og kunnskapsdeling.

Virksomhetene er selv ansvarlig for deteksjon og hendelseshåndtering, og dette må ivaretas av virksomheten selv eller ved kjøp av kapabilitetene som en tjeneste. SRM er ikke direkte involvert i deteksjon med mindre SRM og sektoren/virksomheten spesifikt avtaler det og dermed ønsker å utvide tjenester utover minimumsnivået i modellen, slik som operativ eller rådgivende støtte i hendelseshåndtering. Behovet for dette står SRM fritt til selv å vurdere i samråd med virksomhetene i sektoren.
Ved håndtering av hendelser kan SRM bistå virksomheten med å formidle informasjon fra/til NSM, og eksempelvis via deling av tekniske indikatorer eller annen informasjon som kan støtte virksomheten i håndtering av hendelsen. NSM er ikke direkte involvert i hendelseshåndtering, med mindre hendelsen kan ramme kritisk infrastruktur og/eller kritiske samfunnsfunksjoner.

SRM er ansvarlig for å varsle alle virksomheter sektoren, uavhengig av hvordan SRM er organisert.

Nivå 2 – Avgjørende betydning

Formålet med nivå 2 er å styrke det forebyggende og operative samarbeidet på tvers av sektorer for å sikre samfunnets viktigste funksjoner.

Offentlige og private virksomheter som har avgjørende betydning for grunnleggende nasjonale funksjoner bør inngå i en slik samarbeidsstruktur sammen med NSM og tilhørende SRM der det er tett samhandling mellom aktørene. Ved hendelser av en viss kritikalitet samarbeider aktørene tett på alle områder i hendelseshåndteringen. På dette nivået bør det tilrettelegges for at de samhandlende partene (både SRM og virksomhetene) har tilgang til gradert samhandlingsplattform. Virksomhetene har tilgang til 1:1 dialog med NSM ved behov.

SRM som inngår i dette samarbeidet bør oppfylle noen ytterligere krav i tillegg til nivå 1- og nivå 0 -kravene. Det er hensikten at et SRM skal dekke hele sin sektor, uavhengig av hvilket nivå av krav de oppfyller – men at de på nivå 2 i tillegg skal være i stand til å kunne imøtekomme behovene til virksomheter som har avgjørende betydning for GNF. På dette nivået vil enkelte områder dekkes av sikkerhetsloven. Virksomheter med avgjørende betydning for GNF er underlagt sikkerhetsloven, og dermed eksempelvis pålagt varslingsplikt.

Dette nivået vil være naturlig begrenset i antall SRM og virksomheter, hvilket gjør at man kan opprettholde et høyt tillitsnivå.

NSM, SRM og virksomhetene som inngår i dette samarbeidet bør etablere en samarbeidsavtale som muliggjør deling av informasjon, kapasitet, ressurser ved behov, uten at avtalepartene er forpliktet til å gi fra seg ressurser. Deling av persondata bør reguleres i avtalen slik at det er mulig å dele eksempelvis loggdata ved hendelser.

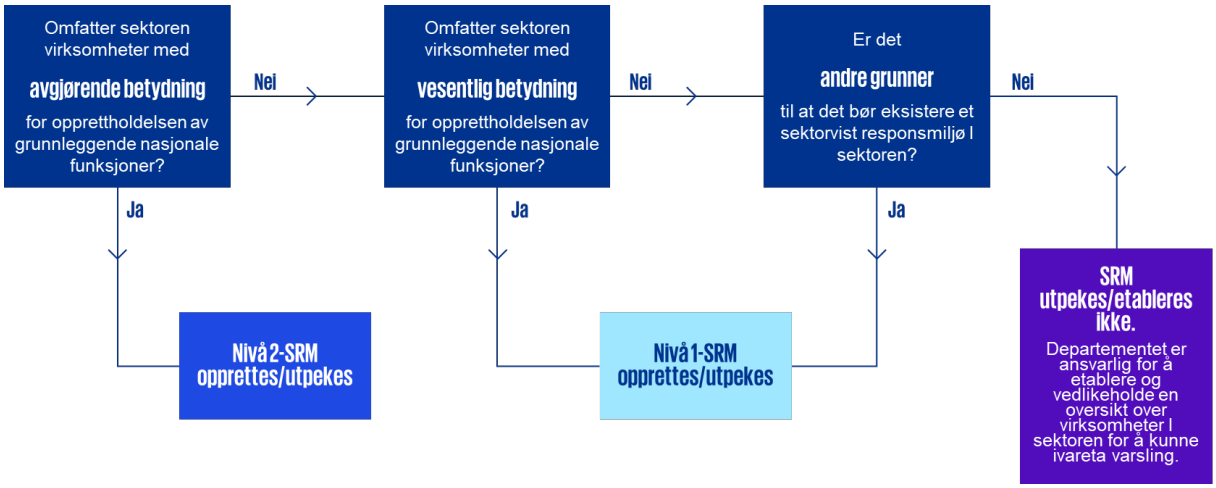
4.1.1 Utpeking av SRM

Hvert departement er ansvarlig for å vurdere hvorvidt sektoren har virksomheter som har vesentlig eller avgjørende betydning for grunnleggende nasjonale funksjoner. KPMGs forslag er å benytte denne prosessen som utgangspunkt for vurdering av eventuelt behov for SRM. I tillegg til at departementene er ansvarlige for vurderingen i sin sektor, anbefaler vi at NSM har en rådgivende funksjon i vurderingen for å sikre en helhetlig oversikt over behovene.

For de sektorene som har virksomheter med avgjørende betydning, utpeker departementet et SRM på nivå 2.

Dersom sektoren ikke har virksomheter med avgjørende betydning for GNF, men har virksomheter med vesentlig betydning eller vurderer at det ellers eksisterer behov for et eget SRM, utpeker departement et SRM på nivå 1.

Dersom departement ikke identifiserer noen virksomheter med avgjørende eller vesentlig betydning, og heller ikke vurderer andre behov for et SRM, kan departement velge å ikke utpeke SRM. I dette tilfellet er departement ansvarlig for å etablere og vedlikeholde en oversikt over virksomheter i sektoren for å kunne ivareta varsling av virksomhetene.



Figur 2 Prosess for utpeking av SRM

Ved behov kan det etableres et felles SRM for sektorene som ikke har behov for og/eller ressurser til et fullverdig SRM alene i sin sektor. Dette «felles-SRM» kan etableres under departementene eller NSM. Hva som er mest hensiktsmessig vil kreve en grundigere vurdering/utredning. Hensikten med anbefalingen er å samle kompetanse og ressurser i store nok fagmiljøer, slik at SRM som minimum har kapasitet til å utføre oppgavene i henhold til de minimumskrav som stilles. Størrelsen på fagmiljøene er også nevnt av SRM som mulig virkemiddel for å ansette og beholde ressurser med riktig kompetanse; i større fagmiljøer er det mulig å sikre faglig utfordrende oppgaver, faglig utvikling og økte muligheter for sparring med kollegaer.

4.1.2 Videreutvikling av rammeverket

En videreutviklet versjon av rammeverket for håndtering av IKT-sikkerhet bør gi et mer helhetlig svar på de utfordringer man står oppe i hva gjelder cybersikkerhet enn det dagens rammeverk gir. Det foreslås å erstatte dagens rammeverk med en «Nasjonal samhandlingsmodell for cybersikkerhet». Formålet med modellen er å tilrettelegge for god tverrsektoriell samhandling. Modellen bør beskrive de ulike aktørenes roller, ansvar og oppgaver. Den bør også beskrive de ulike samhandlingsnivåene, tilhørende kriterier for å inngå i de ulike og kravene som følger av dette.

Det anbefales videre å bytte navn på ordningen fra «sektorvise responsmiljø» til «sektorvis cybersikkerhetssenter». Dette er for at navnet i større grad skal reflektere bredden av tjenester som dagens miljøer leverer, som inkluderer forebyggende oppgaver. Dette innebærer ikke at navnene på dagens etablerte miljøer må endres.

4.1.3 Forutsetninger for en vellykket gjennomføring

I dette avsnittet diskuterer vi forutsetninger for en vellykket gjennomføring. Den helt sentrale forutsetningen for å sikre en vellykket gjennomføring av foreslått modell er å sikre forankring blant de sentrale aktørene som inngår i modellen.

Etter KPMGs vurdering er det særlig avgjørende at forankringen starter i departementsfellesskapet. Særlig viktig er en tett og god dialog mellom JD (sivil sektor) og FD (forsvarssektoren). Som ansvarlig departement på området er det også av kritisk betydning at JD legger til rette for å involvere andre berørte departementer på et tidlig tidspunkt. Det vil også være viktig at ansvaret for gjennomføring tydelig plasseres med nødvendige ressurser og løpende rapportering til JD.

Viktige forutsetninger ved implementering av modellen er en erkjennelse av et trussel- og sårbarhetsbilde i stadig endring og at modellen jevnlig må evalueres og forbedres.

Dernest er det vesentlig å sikre tilstrekkelig involvering av øvrige, berørte aktører. Av Rammeverk for håndtering av IKT-sikkerhetshendelser fremgår at dette er særlig aktuelt for følgende aktører[8]:

- ✓ NSM (herunder FCKS)
- ✓ Politiet (herunder Kripos, PST)
- ✓ Etterretningstjenesten
- ✓ Nasjonal kommunikasjonsmyndighet
- ✓ (Regjeringens kriseråd)
- ✓ SRM
- ✓ CERT og CSIRT-miljøer som ikke har status som SRM
- ✓ Andre myndigheter og etater

I tillegg skal SRM-ordningen først og fremst betjene de virksomheter som inngår i det enkelte SRMs dekningsområde. Som det fremgår av rapporten er behovene for støtte fra SRM-miljøer sterkt varierende mellom sektorer og virksomheter, det samme gjelder tilbudet fra det enkelte SRM. På bakgrunn av dette oppfatter KPMG behov for medvirkning fra virksomhetene som betjenes av SRM for å lykkes med å gjennomføre foreslått modell. Under redegjør vi for vår tenkning knyttet til tidsbruk for gjennomføring av foreslått modell:

- ✓ Ettersom foreslåtte modell vil ha budsjettmessige implikasjoner ut over dagens tilstand (se kapittel 4.2) mener vi at det, basert på erfaring, er rimelig å anta at det vil medgå omtrent ett år på å sikre finansiering.
- ✓ En involveringsprosess som skissert ovenfor vil av erfaring kunne ta inntil ett år, litt avhengig av om det er ønskelig å avgrense involveringsprosessen til departementsfellesskapet og de mest sentrale myndighetsaktørene eller også å inkludere virksomhetene i bred forstand.
- ✓ Et nøkternt anslag med en middels ambisiøs involvering av berørte parter tilsier følgelig en tidshorisont for gjennomføring på to til tre år. Foreslått modell bør følgelig være mulig å gjennomføre fullstendig senest innen 1. juli 2025.

[8] Listen bør oppdateres for å gjenspeile aktørlandskapet slik det er i dag

4.2 Vurdering av administrative og økonomiske konsekvenser

SSBs lønnsstatistikk har vært sentral for våre beregninger. I henhold til statistikken hadde lønnsmottakere i yrke 2529 «Sikkerhetsanalytikere» 67 010 kr i gjennomsnittlig månedslønn i 2021[9]. I beregningene nedenfor er det tatt utgangspunkt i disse lønnskostnadene som tilsvarer en årslønn på om lag 804 000 kroner. Kostnaden for et årsverk er beregnet basert på årslønn pluss 30 % til dekning av arbeidsgiveravgift og andre fastsatte kostnader knyttet til den enkelte ansatte; totalt 1 045 200 per årsverk.

Det er i tillegg lagt til kostnader på 15 000 kr for klient på gradert nett der det vil være aktuelt (gjelder primært ansatte i SRM og virksomheter med avgjørende betydning for GNF på nivå 2 i foreslått modell/alternativ 1). Ettersom det vil tilkomme ekstra kostnader til safer og annen infrastruktur for å håndtere gradert utstyr og informasjon er det lagt til en skjønnsmessig fastsatt kostnad på 10 000 kr per årsverk i tillegg for dekke denne typen kostnader.

Det hefter stor usikkerhet ved beregningene, noe som er illustrert ved det relativt brede kostnadsestimatet. Den største kostnadsdriveren i alternativ 0+ og alternativ 1 vil være knyttet til opprettelsen av nye SRM. Kostnaden vil trolig være mindre ved valg av alternativ 1 enn alternativ 0+ som følge av at en del SRM antakelig ikke blir etablert innenfor rammene av foreslått modell.

4.2.1 Alternativ 0: videreføring av dagens ordning

Til nullalternativet vil det ikke knytte seg økonomiske og administrative konsekvenser ut over dagens situasjon. Alternativet forutsetter at dagens situasjon videreføres. Det vil si at rammeverket for håndtering av IKT-sikkerhetshendelser fortsatt ikke er fullt implementert, herunder at nye SRM ikke utpekes. Dette alternativet er ikke ønskelig med henblikk på å håndtere identifiserte utfordringer (se kapittel 3). Samtidig foreligger det, innen dette alternativet, ikke formelle hindre som umuliggjør nye løsninger for økt og bedre samhandling/deling mellom de ulike SRM og NSM enn dagens situasjon.

KPMG tilrår ikke at dagens situasjon videreføres gitt utfordringene som er beskrevet i kapittel 3.

4.2.2 Alternativ 0+: full implementering av rammeverket

I alternativ 0+ implementeres rammeverket fullstendig slik som det er beskrevet i dag. Viktigst innebærer en full implementering av rammeverket at departementene peker ut SRM i de tilfeller der det ikke er gjort per i dag. KPMG har ikke totaloversikten over hvor mange SRM dette innebærer, men basert på vår kjennskap til sektorer med manglende dekning av SRM kan det være aktuelt å etablere 5-15 nye SRM i tiden fremover. Det typiske SRM har 5-10 årsverk. Ut fra dette vil full implementering av rammeverket innebære følgende mulige økonomiske og administrative konsekvenser:

- ✓ Et sted mellom 25 og 150 nye årsverk i nye SRM (basert på en antakelse om at det vil etableres 10-15 SRM med 5-10 medarbeidere) vil innebære økonomiske konsekvenser i størrelsesordenen fra om lag 52 millioner kroner til 157 millioner kroner.
- ✓ Det er sannsynlig at det, i tillegg til de økonomiske konsekvensene som følger av etableringen av nye SRM, også vil tilkomme kostnader knyttet til økt kapasitetsbehov i NSM for å ivareta nettverket og betjene et større antall SRM. Disse kostnadene er anslått til størrelsesordenen 5-10 millioner kroner.
- ✓ Totalt vil de økonomiske konsekvensene beløpe seg til et sted mellom 57 millioner og 167 millioner kroner ved alternativ 0+.

[9] Ifølge statistikkbankens kildetabell 11418

- ✓ Blant de administrative konsekvensene er det verdt å merke seg at utfordringen knyttet til antallet deltakere i møter og samarbeidsfora vil bli forsterkede.
- ✓ Tendensen til at ressursinnsatsen er for fragmentert i for mange enheter vil tilta.

KPMG anbefaler ikke at dagens rammeverk implementeres fullt ut som følge av at flere opplevde utfordringer med dagens situasjon vil videreføres og forsterkes ved full implementering av det eksisterende rammeverket.

4.2.3 Alternativ 1: KPMGs forslag

Forslaget som beskrevet i kapittel 4.1 innebærer følgende sentrale endringer av dagens ordning:

- ✓ Kravet om at hvert departement må peke ut et SRM erstattes med et minimumskrav til varslingsansvar som kan håndteres av departementet i de tilfeller der det ikke er vurdert hensiktsmessig med et SRM. I noen tilfeller kan dette medføre at SRM ikke blir etablert, men at departementet selv forvalter en kontaktliste for å sikre varsling av virksomheter i egen sektor. Dette vil kunne medføre noe økt arbeidsmengde i enkelte departementer (et sted mellom 0,2 og 0,5 årsverk per departement) som velger denne løsningen.
- ✓ Det etableres to nivåer for samarbeid for SRM, sektornivå og nasjonalt nivå. SRM med tilhørende virksomheter som har avgjørende betydning for GNF, vil få kostnader for klienter og annet utstyr for å få tilgang til gradert samhandling som SRM ikke har i dag.
- ✓ Foreslått modell vil ikke hindre departementene i å utpeke SRM i de tilfeller der det vurderes som en hensiktsmessig løsning. Således vil kostnadsbildet være sammenliknbar med 0+ alternativet selv om det er rimelig grunn til å anta at initiativer til å etablere små SRM med 1-2 ansatte vil blir bremset med dette forslaget.

De viktigste økonomiske og administrative konsekvensene av alternativ 1 følger:

- ✓ For SRM med virksomheter som har avgjørende betydning for GNF, samt disse virksomhetene, vil det påløpe kostnader knyttet til tilgang til gradert plattform. Kostnadene for gradert samhandling anslås til 25.000 kroner per årsverk, inkludert kostnader knyttet til utstyr for å håndtere gradert informasjon er skjønnsmessig fastsatt[10].
  - Vår foreløpige vurdering er at SRM i nivå 2 vil inkludere 6-8 SRM i dagens ordning.
  - For aktuelle SRM i disse sektorene vil tilgang til gradert samhandling innebære en kostnad på om lag 750 000 – 2 000 000 kroner[11].
- ✓ Som følge av at foreslått modell ikke endrer muligheten til å peke ut nye SRM vil det også innen rammene av modellen tilkomme nye SRM. Det er imidlertid vår vurdering at de minste, SRM ikke vil bli etablert og/eller håndtert av ansvarlig departement. Det antas at dette vil medføre noe lavere økonomiske konsekvenser enn 0+ alternativet (etablering av 4-8 nye SRM med 5-10 ansatte). De økonomiske konsekvensene av nye SRM vil dermed være i størrelsesordenen om lag 21 millioner kroner til 84 millioner kroner.
- ✓ I tillegg vil de departementer som ikke utpeker SRM selv måtte ajourføre varslingsliste og eventuelt varsle virksomheter i sin sektor ved hendelser. Dette anses å være en relativt avgrenset arbeidsoppgave som bør kunne løses innenfor rammen av inntil 0,2 årsverk per departement. Det antas at inntil 10 departementer vil kunne ha behov for å ivareta slike lister for deler av sektoren som ikke er dekket av et SRM, eller for hele sektoren der det eventuelt vurderes som unødvendig med et SRM. Anslåtte kostnader blir dermed mellom 0 og 2 millioner kroner.
- ✓ Behovet for styrking av NSM vurderes likt som i alternativ 0+ og settes til 5-10 millioner kroner.

[10] Dersom virksomheten allerede har tilgang til NBN trenger de ikke å få det på nytt. KPMG er ikke kjent med omfanget av slike tilfeller og det er derfor ikke hensyntatt i våre overslag.

[11] Ansatte i forsvaret har allerede tilgang til gradert samhandling og er ikke hensyntatt i regnestykket.

- ✓ De totale økonomiske konsekvensene av alternativ 1 er dermed innenfor spennet 27 millioner kroner og 98 millioner kroner. Anslåtte, maksimale økonomiske konsekvenser er dermed noe lavere enn for alternativ 0+.
- ✓ Alternativ 1 vil medføre en økt ressursinnsats, muligheter for deling og økt samhandling mellom utpekte SRM på nivå 2. Samtidig er det rimelig å anta at det vil utpekes færre SRM i sektorer med avgrenset behov for responsmiljøer og at en derigjennom kan begrense ressursbruken på små SRM og samtidig oppnå en mer hensiktsmessig ressursbruk med større fagmiljøer som har større dekningsområde.

Vedlegg

Appendix 1 FIRST CSIRT Services Framework v2.1

I rapporten henvises til rammeverket «FIRST CISRT Services Framework v2.1».

First (Forum of Incident Response and Security Teams) er en global anerkjent organisasjon, og ledende innen hendelsesrespons. FIRST tilrettelegger for at responsmiljø responderer mer effektivt på sikkerhetstruende hendelser og effektivt oppdager og håndterer kritiske sårbarheter. Organisasjonen er et forum for klarerte responsmiljøer og stiller tydelige krav til medlemsorganisasjonene. Sammen utvikler og deler FIRST teknisk informasjon, verktøy, metodikk, prosesser og beste praksis.

«CSIRT Services Framework» er et rammeverk som på en strukturert måte beskriver de funksjoner og tjenester som ofte ivaretas og leveres av operative IKT-sikkerhetsfunksjoner (CSIRT, SOC eller CERT). Rammeverket er utarbeidet av anerkjente eksperter fra sikkerhetsbransjen (tilknyttet FIRST), med støtte fra Task Force CSIRT (TF-CSIRT) og International Telecommunications Union (ITU).

Formålet med rammeverket er å støtte arbeidet med etablering og videreutvikling av operative IKT-sikkerhetsfunksjoner, med spesielt fokus på innledende fase der det arbeides med valg, utvidelse og styrking av tjenesteporteføljen. Tjenestene som beskrives er i all hovedsak alle de tjenestene som en operativ IKT-sikkerhetsfunksjon kan levere. En operativ IKT-sikkerhetsfunksjoner er ikke forventet å levere alle tjenestene i rammeverket, men enhver CSIRT, SOC eller CERT velger de tjenestene som best understøtter måloppnåelse sett i lys av eget oppdrag og egne forutsetninger.

Tjenestene i rammeverket skal bidra til å forebygge, detektere, håndtere IKT-sikkerhetshendelser og sårbarheter. Tjenestekategoriene er som følger:

- ✓ Deteksjon
- ✓ Hendelseshåndtering
- ✓ Sårbarhetshåndtering
- ✓ Situasjonsforståelse
- ✓ Kunnskapsdeling

Disse tjenestekategoriene inneholder videre et sett med tjenester som illustrert i figur X[12]:

Figur 3 Illustrasjon av tjenestene i FIRST CSIRT Services Framework

[12] KPMG gjør oppmerksom på at de norske benevningene i figuren er oversatt av KPMG og ikke verifisert av FIRST.

Appendix 2 Intervjuoversikt

Dato	Organisasjon	Deltakere
24.5.2022	Nettverk for digital sikkerhet	Bjørn Astad, Trine-Lise Waldorff, Katarina de Brisis, Gard Kjølholdt, Mia Thore Ronde Harlyng, Torill A. Østrem Tørlen, Gustav Birkeland, Lasse Gråberg, Aino von Düring, Jarl-Andre Skarsten, Hilde Goutal Müller, Ola Berge, Kristine Wennberg, Kenneth Jacobsen
24.5.2022	MiljøCERT	Ågot Marianne Stornes
24.5.2022	NFCERT	Morten Tandle
30.5.2022	KraftCERT	Margrete Raaum, Martin Bore
30.5.2022	Kommune-CSIRT	Bjørn Tveiten
31.5.2022	HelseCERT	Gunnar A. Johansen
01.06.2022	JustisCERT	Berit Schmidt, Oddvar Kaaby, Stian Kristoffersen
03.06.2022	CSS	Cecilie Østlund Hammer
17.06.2022	Equinor, Hydro	Lars Idland, Torstein Gimnes Are
20.06.2022	NSM, NVE	Harald Kristian Næss, Janne Merete Hagen
20.06.2022	NSM	Øivind Mandt, Svenn Richard Andersen
21.06.2022	NSM	Svenn Richard Andersen, August Verholdt
22.06.2022	SRM	Morten Tandle, Bjørn Tveiten, Mike Andersen, Margrete Raaum, Berit Schmidt, Frank Stien, Cecilie Østlund Hammer, Oddvar Kaaby, Rune Sydskjør, Gunnar A. Johansen
21.06.2022	NSM	Truls Campe Pettersen, Mari Kvaal
21.06.2022	Justisråd ved EU-delegasjonen	Josefine Aaser
22.06.2022	Den norske ambassaden i Washington DC.	Samfunnssikkerhetsråd Per Kristen Brekke

Appendix 3 Om NIS 2 -direktivet

Formålet med NIS 2 -direktivet er å styrke motstandsdyktighet gjennom effektivt samarbeid mellom myndighetene i medlemsstatene. Forslaget til nytt direktiv øker dekningsområdet sammenlignet med det nåværende direktivet ved å utvide antall sektorer som defineres som kritiske. Direktivet vil skille mellom to kritikalitetsnivåer, «vesentlig» og «viktig». Sektorer som i forslaget defineres som «vesentlig» er for eksempel energi, transport, bank, finansmarkedsinfrastrukturer, helse, drikkevann, avløpsvann, digital infrastruktur, offentlig forvaltning og romvirksomhet[13].

Forslaget for videreutvikling av ordningen med sektorvise responsmiljøer i denne rapporten er knyttet til prosessen å definere grunnleggende nasjonale funksjoner. Utvalget av «vesentlige» sektorer i forslaget til NIS 2 -direktiv er noe bredere enn identifiserte GNF på tidspunkt denne rapporten ble skrevet. Det viktigste i forholdet mellom NIS 2 -direktivet og ordningen med sektorvise responsmiljøer blir å avgjøre forholdet mellom NIS 2 -direktivet og identifiserte GNF, og vurdere om sektorer som defineres som «vesentlig» i NIS 2 -direktivet vil resultere i flere GNF og dermed flere virksomheter som har avgjørende betydning for GNF. Samtidig vil NIS 2 -direktivet innføre avgrensninger mot mindre virksomheter slik at det kun vil være større virksomheter som blir underlagt NIS 2 -direktivet. Dermed kan det antas at antall virksomheter som i forslaget i denne rapporten inkluderes i Nivå 2 Avgjørende, ikke nødvendigvis øker betydelig som følge av NIS 2 -direktivet.

[13] NIS2 - direktivet - regjeringen.no

Kontakt oss:

Hans Christian Pretorius
Partner
T +47 90879077
E **hans.christian.pretorius@kpmg.no**

kpmg.no