Rammeverk for håndtering av IKT-sikkerhetshendelser

Versjon per 07.12.17

Innhold

1 Innledning

1.1 Bakgrunn

Det er i Norge en økende erkjennelse av at vi som et sterkt digitalisert og åpent demokratisk samfunn lever med risiko for at det kan inntreffe alvorlige IKT-sikkerhetshendelser. Risikoen knytter seg særlig til tre forhold: 1) flere og mer komplekse systemer er bærere av funksjoner og tjenester (verdier) vi er avhengige av i samfunnet; 2) vi opplever stadig flere angrep, stadig mer raffinerte angrepsmetoder og stadig mer ressurssterke aktører; og 3) det er en sterkere avhengighet mellom virksomheter som understøtter kritisk infrastruktur og kritiske samfunnsfunksjoner, og lengre og mer uoversiktlige verdikjeder.

Det er ikke mulig å eliminere denne risikoen – angrep vil inntreffe og enkelte av disse vil være vellykkede sett fra angriperens side. En velfungerende koordinert innsats for å fange opp indikasjoner på angrep, minimere skade, redusere konsekvenser, gjenopprette sikker drift, samt etterforske IKT-sikkerhetshendelser vil være viktig fremover på alle nivåer i samfunnet for å redusere risikoen. Slik motstandskraft mot alvorlige IKT- sikkerhetshendelser etableres gjennom effektiv ressursbruk i et samspill mellom virksomhetene, sektorene og det nasjonale sektorovergripende nivået.

1.2 Formål

Nasjonal håndtering av IKT-sikkerhetshendelser

Formålet med rammeverket for håndtering av IKT-sikkerhetshendelser er:

- å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon om alle relevante IKT-sikkerhetshendelser
- å effektivt håndtere alvorlige IKT-sikkerhetshendelser fra virksomhetsnivå til politisk nivå gjennom god utnyttelse av samfunnets samlede ressurser
- at Norge fremstår koordinert overfor andre land og internasjonale organisasjoner

Med håndtering av IKT-sikkerhetshendelser menes i dette rammeverket defensive prosesser og tiltak for å detektere (avdekke) og stanse alvorlige IKT-sikkerhetshendelser, samt å gjenopprette sikker tilstand for berørte systemer, skadevurdere og skadebegrense.

Med alvorlige IKT-sikkerhetshendelser menes tilsiktede uønskede hendelser eller trusler om slike hendelser i det digitale rom som er rettet mot kritisk infrastruktur og/eller kritiske samfunnsfunksjoner.

Målgruppe

Målgruppen for rammeverket for håndtering av IKT-sikkerhetshendelser er offentlige og private virksomheter som har betydning for kritisk infrastruktur og/eller kritiske samfunnsfunksjoner[1], sektorvise responsmiljøer (SRM), myndigheter som har en rolle knyttet til håndtering av IKT-sikkerhetshendelser og departementer.

Rammeverket vil også kunne ha nytteverdi for virksomheter som ikke har betydning for kritisk infrastruktur og/eller kritiske samfunnsfunksjoner, virksomheter som tilbyr IKT-tjenester og -produkter til tredjepart, og for respons-, CERT[2]- og CSIRT[3]-miljøer som ikke har status som SRM.

Rammeverk for håndtering av IKT-sikkerhetshendelser

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. De etablerte beredskapsprinsippene legges til grunn.[4] Rammeverket beskriver også de forutsetningene som må være på plass for at håndtering av IKT-sikkerhetshendelser skal kunne foregå i henhold til rammeverket. Forholdet til andre elementer i en mer omfattende hendelseshåndtering, eksempelvis etterforskning, beskrives i den grad det er nødvendig for helhetsforståelsen. Målet er at den enkelte virksomhet som forvalter kritisk infrastruktur og/eller kritiske samfunnsfunksjoner[5] skal utøve sin rolle og sitt ansvar raskt og formålseffektivt som del av en større, koordinert respons for å gjenopprette sikker tilstand for berørte systemer, utføre skadevurdering og begrense følgeskader for andre IKT-systemer. Dette inkluderer informasjonssystemer som håndterer sikkerhetsgradert informasjon. Rammeverket forutsetter at den enkelte virksomhet utarbeider egne detaljerte planer for håndtering av alvorlige IKT-sikkerhetshendelser som henger sammen med øvrig beredskapsplanverk.

Håndtering av IKT-sikkerhetshendelser reguleres i Norge i dag gjennom flere sektorovergripende eller sektorspesifikke lover og forskrifter.[6] Rammeverket erstatter ikke eventuelle føringer om hendelseshåndtering i disse regelverkene. Slike føringer må det derfor tas hensyn til når den enkelte virksomhet utvikler detaljerte planer.

Rammeverket er anvendelig i hele konfliktspennet fra alvorlige enkelthendelser i enkeltsektorer, til nasjonale, tverrsektorielle kriser, sikkerhetspolitiske kriser og væpnet konflikt. Rammeverket

[1] DSBs rapport «Samfunnets kritiske funksjoner»(2016) redegjør for virksomheter som har betydning for kritisk infrastruktur og samfunnskritiske funksjoner.
[2] Computer Emergency Response Team
[3] Computer Security Incident Response Team
[4] Arbeidet med samfunnssikkerhet og beredskap tar utgangspunkt i etablerte prinsipper for krisehåndtering; ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet og samvirkeprinsippet. Se Meld. St. nr. 10 (2016-2017) *Risiko i et trygt samfunn - Samfunnssikkerhet*
[5] Se Meld. St. nr. 22 (2007-2008) *Samfunnssikkerhet,* og DSBs rapport *«Samfunnets kritiske funksjoner»* (2016).
[6] Relevante lover og forskrifter i denne sammenheng er blant andre Lov om forebyggende sikkerhet (sikkerhetsloven) med forskrifter, Lov om behandling av personopplysninger (personopplysningsloven) med forskrift, Lov om elektronisk kommunikasjon (ekom-loven), Straffeloven, Politiregisterloven, Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven), Lov om arkiv (arkivloven), Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven), Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) og Forskrift om offentlige arkiv (arkivforskrifta).

kommer ikke i konflikt med tiltak i Nasjonalt beredskapssystem (NBS) som vil kunne bli iverksatt ved store alvorlige hendelser.

På et tidlig stadium kan det være uklart om en hendelse skyldes en tilsiktet handling eller en utilsiktet feil, ulykke eller liknende. Rammeverket gjelder inntil dette er avklart og dersom årsaken til hendelsen viser seg å være en tilsiktet handling.

Rammeverket omfatter hendelseshåndtering på alle nivåer, men skal ikke gripe inn i politiske, strategiske eller departementale prosesser. Rammeverket kan imidlertid gi innspill til slike prosesser. I den grad rammeverket omfatter relasjonene til andre land eller internasjonale organisasjoner, skal slik kontakt være knyttet til håndtering av IKT-sikkerhetshendelser.

Rammeverket erstatter "Modell for håndtering av IKT-hendelser" utgitt av Justis- og beredskapsdepartementet i 2014.

1.3 Avgrensning

Politiets oppgaver

De fleste hendelsene som dette rammeverket dekker, kan eller bør bli gjenstand for etterforskning. Rammeverket omtaler ikke prosessen knyttet til etterforskning, men beskriver forholdet mellom håndtering av IKT-sikkerhetshendelser og etterforskning. Alle straffbare forhold i det digitale rom bør meldes til politiet, på samme måte som andre straffbare forhold. Politiet plikter her som ellers å bistå enkeltpersoner og virksomheter, skape trygghet for befolkningen i alminnelighet og kritisk infrastruktur og kritiske samfunnsfunksjoner i særdeleshet, og eventuelt etterforske forholdet.[7]

Etterretningstjenestens oppgaver

Rammeverket gjelder ikke offensive operasjoner i det digitale rom, som ligger under Etterretningstjenestens ansvarsområde overfor utenlandske mål. Rammeverket omfatter heller ikke Etterretningstjenestens oppgave med å innhente etterretning om utenlandske forhold. Til informasjon for brukere av rammeverket vil det likevel henvises til Etterretningstjenesten enkelte steder, særlig om tjenestens samarbeid med andre nasjonale aktører og om tjenestens ugraderte etterretningsvurderinger.

Håndtering av konsekvenser

Rammeverket omfatter ikke håndtering av konsekvenser av IKT-sikkerhetshendelser. Slik håndtering følger av regelverk og andre beredskapsrutiner. For å minimere konsekvenser er det viktig at politiet og andre relevante aktører med ansvar for hendelseshåndtering varsles så fort som mulig i henhold til de alminnelige etablerte rutiner og regelverk.

Dersom det oppstår svikt i kritisk infrastruktur eller kritiske samfunnsfunksjoner på grunn av IKT-sikkerhetshendelser, vil det medføre behov for krisehåndtering av en rekke aktører, som

[7] Dette gjelder plikter og hjemler i henhold til politiloven til å forebygge, avdekke og stanse angrep og skade – om nødvendig ved bruk av maktmidler. Det gjelder også plikter og hjemler etter straffeprosessloven til å avdekke, etterforske og avverge straffbare forhold, om nødvendig ved bruk av tvangsmidler.

beredskapsetater, kommuner eller frivillige organisasjoner, tilsvarende som for andre hendelser som rammer kritiske samfunnsfunksjoner. Håndtering i tråd med dette rammeverket skal ikke erstatte det ordinære krisehåndteringsapparatet, men kommer i tillegg.

Privatpersoner

Rammeverket gjelder ikke for hendelser som rammer privatpersoner. Håndtering av tilsiktede handlinger som rammer privatpersoner, følger av eget lovverk.

1.4 Forvaltning av rammeverket

Rammeverket fastsettes av Justis- og beredskapsdepartementet for sivil sektor og Forsvarsdepartementet for forsvarssektoren.

Rammeverket er dynamisk og skal revideres hvert annet år, eller hyppigere ved behov.[8] Nasjonal sikkerhetsmyndighet (NSM) er ansvarlig for revisjonsprosessen og vurderer behov for endringer. Revisjoner fremlegges departementene for godkjenning. NSM skal sikre involvering av sentrale aktører i forbindelse med revisjon.

Innspill om behov for endringer i rammeverket skal fremsendes til NSM fortløpende.

2 Myndighetsansvar og hjemmelsgrunnlag i det digitale rom

2.1 Regjeringen

Regjeringen har det øverste ansvaret for nasjonal sikkerhet og beredskap, herunder det overordnede politiske ansvaret for både styringen og håndteringen av forebyggende arbeid og enkeltstående kriser som oppstår. Dette gjelder også ved håndtering av IKT-sikkerhetshendelser.

2.2 Departementene

Den enkelte statsråd har det konstitusjonelle ansvaret på sitt område, innenfor de lover og bevilgninger Stortinget har gitt. Dette ansvaret gjelder også for forebyggende IKT-sikkerhet og håndtering av IKT-sikkerhetshendelser i sektoren i normalsituasjoner og i kriser. Ved kriser må departementene innhente situasjonsrapporter fra egne operative virksomheter og være i stand til å identifisere og treffe beslutninger om nødvendige tiltak innen eget ansvarsområde for å håndtere den aktuelle situasjonen. Departementene skal påse at operative aktører har nødvendige fullmakter og vurdere behov for nasjonal og/eller internasjonal bistand til egen sektor. Departementene må videre kunne håndtere kommunikasjon med medier og befolkningen. Arbeidet må skje koordinert med andre departementer.

Kriserådet skal styrke den sentrale krisekoordineringen mellom departementene og er det overordnede administrative koordineringsorgan. Justis- og beredskapsdepartementet er fast lederdepartement i Kriserådet ved sivile nasjonale kriser, dersom Kriserådet ikke bestemmer noe

[8] Forhold som kan tilsi hyppigere revisjon er eksempelvis endringer i nasjonale krav, erfaringer fra øvelser og håndtering av IKT-sikkerhetshendelser.

annet. Krisestøtteenheten er permanent sekretariat for Kriserådet og skal støtte lederdepartementet.

Departementene skal påse at det er etablert sektorvise responsmiljøer (SRM) med operativt ansvar for å dekke virksomheter innen hele eller deler av departementets myndighetsområde.[9]

Forsvarsdepartementet

Forsvarsdepartementet (FD) har ansvar for utforming og iverksetting av norsk sikkerhets- og forsvarspolitikk.

FD har ansvar for alt arbeid med forebyggende IKT-sikkerhet knyttet til forsvarssektoren og forvaltningsansvaret for sikkerhetsloven. FD har ansvaret for den strategiske ledelsen og styringen av Forsvaret, NSM og de øvrige etatene i sektoren.

Justis- og beredskapsdepartementet

Justis- og beredskapsdepartementet (JD) har et samordningsansvar for samfunnssikkerhets- og beredskapsarbeidet i sivil sektor. JD har videre i henhold til kgl.res. 22. mars 2013 og kgl.res. 10. mars 2017, også et samordningsansvar for IKT-sikkerhet i sivil sektor. Dette omfatter utforming av en nasjonal politikk og nasjonale krav for IKT-sikkerhet. Slike krav vil kunne omfatte både offentlig og privat sektor. For det siste kreves hjemmel i lov.

FD og JD har det overordnede ansvar for forebyggende sikkerhet i medhold av sikkerhetsloven i henholdsvis forsvarssektoren og sivil sektor.

2.3 Sentrale myndigheter, etater og organer

2.3.1 Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) er fag- og tilsynsmyndighet etter lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). Etter lovens § 8 skal NSM koordinere forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden.

Sikkerhetslovens § 9 første ledd tillegger NSM det nasjonale ansvaret for å koordinere håndtering av alvorlige IKT-sikkerhetshendelser mot kritisk infrastruktur. Som ledd i denne virksomheten skal NSM etter loven etablere og drive et varslingssystem som kan detektere IKT-sikkerhetshendelser mot kritisk infrastruktur. NSM skal gjennom sin virksomhet innhente, verifisere, analysere og videreformidle informasjon om sårbarheter, potensielle risikoer, metoder og ondsinnet kode, samt koordinere og bistå i håndteringen av alvorlige IKT-sikkerhetshendelser med formål om å gjenopprette systemenes sikre tilstand. I lovens forarbeider er det lagt til grunn at denne oppgaven skal utøves i et nært samspill med Politiets sikkerhetstjeneste, Etterretningstjenesten og Kripos, og at det også skal samarbeides med sektorvise responsmiljøer (SRM) og andre relevante aktører.

[9] Føringer om slik etablering er gitt i Meld. St. 29 (2011-2012) Samfunnssikkerhet, pkt. 4.4., og gjentatt i Nasjonal strategi for informasjonssikkerhet (2012), pkt. 4.4, med tilhørende handlingsplan, tiltak 4.2.

Som et ledd i den nasjonale koordineringen av hendelser utgir NSM retningslinjer for samhandling mellom SRM og NSM.

2.3.2 Etterretningstjenesten

Etterretningstjenesten har et sektorovergripende ansvar på nasjonalt nivå i fred, krise og væpnet konflikt for blant annet å avdekke utenlandske trusler og frembringe etterretninger om fremmede trusselaktører i det digitale rom, samt ansvar for andre offensive cyberoperasjoner (inkludert aktive forsvarsoperasjoner) mot fremmede mål innenfor rammen av folkeretten og norsk lov.

2.3.3 Politiet

Politiets hovedoppgaver er å opprettholde alminnelig lov og orden, forebygge og forhindre straffbare handlinger, beskytte borgerne og deres lovlydige virksomhet samt etterforske lovbrudd. Politiet har også ansvar for organisering av redningsinnsatsen ved ulykker, kriser og andre uforutsette hendelser, og utfører forvaltningsoppgaver.

I politiloven § 2 tillegges politiet oppgaver knyttet til den alminnelige tryggheten i samfunnet. I dette ligger det en plikt til, innen alle områder, å arbeide forebyggende, yte hjelp, og å bistå andre offentlige myndigheter i deres oppgaver og tjenesteutøvelse.

Politiloven § 27 pålegger politiet en plikt til å iverksette tiltak for å redde menneskeliv, og innebærer at politiet skal ha beredskap for å ta ansvar i alle ulykkes- og katastrofesituasjoner. Dette gjelder også når utgangspunktet for slike situasjoner ligger i det digitale rom.

Politiet har monopol på bruk av makt i Norge og enerett til å bruke maktmidler overfor borgerne. Politiet kan f.eks. nedlegge forbud, gi pålegg og gjennomføre relevante tvangstiltak når situasjonen gjør det nødvendig. Dette gjelder også når forholdene skjer i det digitale rom eller ved digitale metoder. Fullmaktene gjelder uavhengig av om det foreligger mistanke om straffbare forhold. De gir politiet hjemmel til å iverksette tiltak for å forhindre og stanse straffbare forhold og til å redusere skade. Når politiet har iverksatt etterforskning, har de særlige hjemler i straffeprosessloven til å iverksette tiltak for å innhente informasjon og for å avverge nye straffbare forhold, også ved skjulte tvangsmidler når det er nødvendig.

Ved etterforskning er politiet i påtalespørsmål underlagt overordnet påtalemyndighet. Både PST og Kripos er underlagt Det nasjonale statsadvokatembetet (NAST).

Politiets sikkerhetstjeneste (PST)

PST er et politiorgan og Norges innenlandske sikkerhets- og etterretningstjeneste, direkte underlagt Justis- og beredskapsdepartementet. PST skal beskytte demokratiet, borgerne og vitale samfunnsinteresser gjennom å avdekke, forebygge og etterforske spionasje, terror, spredning av masseødeleggelsesvåpen og trusler mot myndighetspersoner. Det er også en viktig oppgave for PST å utarbeide analyser og trusselvurderinger til bruk som beslutningsunderlag både for egen forebyggende virksomhet og for overordnede organ og andre som har behov for denne type informasjon. PST har ulike hjemler for å innhente informasjon avhengig av formålet med informasjonsinnhentingen. De har herunder hjemler til å benytte skjult informasjonsinnhenting i forebyggende saker – på strenge vilkår.

PST er, som politiet for øvrig, styrt av politiloven og straffeprosessloven. Særlige bestemmelser som beskriver PSTs ansvarsområde fremgår av politiloven kapittel III a.

Kripos

Kripos er den nasjonale enheten for bekjempelse av organisert og annen alvorlig kriminalitet, inkludert datakriminalitet, og er underlagt Politidirektoratet. Enheten har spisskompetanse innen kriminaletterretning og taktisk og teknisk datakrimetterforskning. Kripos har en egen datakrimenhet som driver etterretning, forebygging, avdekking og etterforskning, samt bistår det øvrige politiet og overordnet påtalemyndighet. Enheten for internett-relatert etterforskningsstøtte bistår med sikring av elektroniske spor og bevis på internett, utlevering fra tjenestetilbydere, ransakinger, analyse av beslag, mv.

2.3.4 Felles cyberkoordineringssenter

Felles cyberkoordineringssenter (FCKS) består av NSM, Etterretningstjenesten, PST og Kripos, og ledes av NSM. Formålet med FCKS er å styrke nasjonal evne til effektivt forsvar mot og håndtering av alvorlige hendelser og kriminalitet i det digitale rom. FCKS er et permanent og samlokalisert fagmiljø, bestående av faste representanter fra hver av partene. Senteret er ikke et selvstendig organ med egen beslutningsmyndighet.

Virkeområdet til FCKS er alvorlige hendelser i det digitale rom. FCKS skal koordinere partenes innsats ved håndtering av hendelser, herunder bidra til mer effektiv bruk av nasjonale ressurser, styrke informasjonsdeling, samt ivareta koordinert varsling til og frembringelse av helhetlige beslutningsgrunnlag til overordnede myndigheter. Senteret representerer ikke en kapasitet hvor virksomheter kan henvende seg for bistand til håndtering.

2.3.5 Nasjonal kommunikasjonsmyndighet

Nasjonal kommunikasjonsmyndighet (Nkom) er tilsynsmyndighet for virksomheter som tilbyr post- og ekomtjenester. Nkom er underlagt Samferdselsdepartementet.

Som en del av myndighetsarbeidet jobber Nkom med å stille krav til og føre tilsyn med sikkerhet og beredskap i offentlige elektroniske kommunikasjonsnett og -tjenester. Nkom er ansvarlig for myndighetsutøvelsen i forbindelse med hendelseshåndtering innen ekomsektoren og for forvaltning av taushetsplikt i post- og ekomsektoren. Ekomsektorens SRM, EkomCERT, ligger organisatorisk til Nkom.

Nkom arrangerer jevnlige møter i Ekom sikkerhetsforum, en sikkerhetsfaglig møtearena for sentrale ekomtilbydere[10], Nkom, Etterretningstjenesten, PST og NSM. I dette forumet deles sårbarhets- og trusselinformasjon på gradert nivå opp til HEMMELIG. I tillegg til de jevnlige møtene kan Ekom sikkerhetsforum kalles inn på kort varsel, enten med alle til stede eller med et mindre utvalg ekomtilbydere og myndighetsorganer.

2.3.6 Andre myndigheter og etater

Ulike sektormyndigheter og regelverksforvaltere har utøvende ansvar og roller, herunder hjemler til å kreve rapportering fra virksomheter og hjemler til å iverksette tiltak.

[10] Pr 10.7.2017 er Telenor, Telia, Ice, Broadnet, Cyberforsvaret og Nødnettet (DSB/NBK) oppnevnt som medlemmer i forumet. Sammensetningen endres ved behov.

3 Håndtering av IKT-sikkerhetshendelser

IKT-sikkerhetshendelser som faller inn under rammeverkets virkeområde skal håndteres gjennom en systematisk prosess bestående av 1) planlegging og forberedelse; 2) deteksjon og vurdering av omfang og alvorlighetsgrad; 3) varsling av relevante parter; 4) iverksetting av prosesser og tiltak for å håndtere hendelsen; 5) situasjonsrapportering og 6) tilbakeføring og læring av hendelsen.[11] Prosessen er gjennomgående for de tre nivåene som rammeverket bygger på: a) virksomheter/systemeiere, b) sektorvise responsmiljøer (SRM) med fullmakt fra departement og c) NSM på nasjonalt sektorovergripende nivå. Prinsippskissen for håndtering av IKT-sikkerhetshendelser i vedlegg 1 gir en illustrasjon av forholdet mellom nivåene. Nedenfor beskrives prosessene mer detaljert for de tre nivåene.

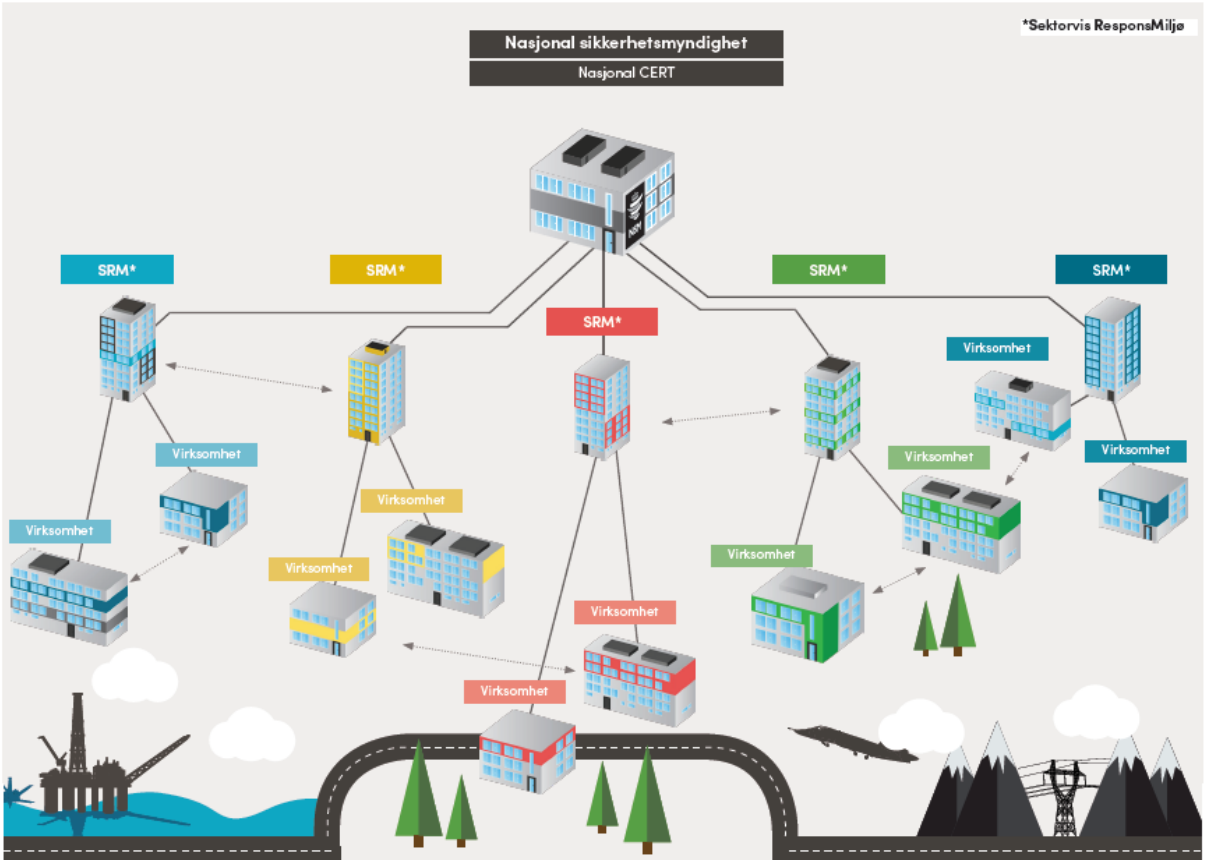
Departementene er ansvarlige for å oppnevne SRM i sektorene og for å sikre at SRM til enhver tid oppfyller gjeldende krav og forventninger som stilles til denne funksjonen.[12] Det enkelte departementet har stor fleksibilitet knyttet til å vurdere hvorvidt det er hensiktsmessig med ett eller flere SRM i egen sektor, eller om det for noen sektorer kan være hensiktsmessig med tverr-sektorielle SRM.

I påvente av at departementene oppnevner SRM for sin(e) sektor(er), vil departementet selv måtte ivareta oppgavene som påhviler SRM slik det fremkommer her i kapittel 3 i rammeverket. Departementene er videre ansvarlig for at virksomheter som har betydning for kritisk infrastruktur og kritiske samfunnsfunksjoner er identifisert i sektoren slik at de er forberedt på å følge opp de oppgavene som følger av rammeverket, og se til at disse er beskyttet av tilfredsstillende grunnsikring.

IKT-sikkerhet er først og fremst den enkelte virksomhets ansvar. Dette følger av ansvarsprinsippet, som innebærer at den som har et ansvar for en virksomhet under normale forhold, også har et ansvar i en krisesituasjon. I praksis innebærer dette at ansvaret for å håndtere IKT-sikkerhetshendelser ligger hos eier av virksomheten, uavhengig av om denne befinner seg i privat eller offentlig sektor.

[11] Prosessen er i overensstemmelse med ISO 27001

[12] Dette med bakgrunn i føringer gitt i Meld. St. 29 (2011-2012) Samfunnssikkerhet, pkt. 4.4., og gjentatt i Nasjonal strategi for informasjonssikkerhet (2012), pkt. 4.4, med tilhørende handlingsplan, tiltak 4.2.



Figur 1 – Kommunikasjon mellom NSM, SRM og virksomheter i og mellom sektorer

3.1 Planlegging og forberedelse

Planlegging og forberedelse dreier seg om å etablere prosedyrer for håndtering av hendelser, inkludert rapportering, ansvarslinjer og eskaleringsrutiner og etablering av et IKT-risikobilde.

Det forutsettes at virksomheter som omfattes av rammeverket har implementert en grunnsikring[13] basert på egne risiko- og sårbarhetsvurderinger.[14] Robuste systemer er et viktig premiss for å motstå IKT-sikkerhetshendelser.

3.1.1 Forventninger til aktører knyttet til planlegging og forberedelse

Virksomheter forutsettes å:

- motta, vurdere og formidle informasjon fra og til eget SRM
- ha systemer for loggføring av nettverkstrafikk
- delta i samhandlingsøvelser
- ha beredskapsplaner for håndtering av større hendelser og sikkerhetspolitiske kriser i det digitale rom

[13] Se NSMs veileder «*Grunnprinsipper for IKT-sikkerhet*», 2017. Sektorregelverk eller andre bestemmelser kan stille ytterligere krav til grunnsikring.

[14] Risiko- og sårbarhetsanalyse er en strukturert vurdering av 1) hvilke uønskede hendelser som kan komme til å skje, 2) sannsynlighet for at en uønsket hendelse vil inntreffe, 3) sårbarhet ved systemer sannsynlighet og konsekvens, 4) hvilke konsekvenser hendelsen eventuelt vil få og 5) usikkerheten knyttet til vurderingene

- oppdatere seg gjennom relevante utredninger og årlige og løpende trusselvurderinger rettet mot det digitale rom [15]
- gjennomføre jevnlige risikovurderinger for egen virksomhet rettet mot det digitale rom
- oppdatere kontaktinformasjon og melde inn endringer til eget SRM

Sektorvise responsmiljøer skal:

- etablere og vedlikeholde sambandskatalog og aktørkart for sektoren, og melde dette inn til NSM[16]
- etablere rutiner for bruk av kryptert kommunikasjon i sektoren
- kunne sende og motta gradert informasjon i henhold til sektorens behov
- ha sikkerhetsklarert og autorisert personell på nødvendig nivå i henhold til sektorens behov
- ha kunnskap om departementet/enes oversikt over kritisk infrastruktur og kritiske samfunnsfunksjoner i sektor
- avklare rutiner for deling av hendelses- og risikoinformasjon i sektor, på tvers av sektorer og mot NSM
- delta i samhandlingsøvelser i og utenfor sektor
- ha et saksbehandlingssystem hvor elektronisk kommunikasjon kan kategoriseres, lagres og gjenfinnes. Dersom systemet behandler informasjon som er sikkerhetsgradert, skal systemet være sikkerhetsgodkjent som gradert informasjonssystem
- arrangere møter for erfaringsutveksling og samhandling for virksomheter i sektor
- ha oversikt over miljøer med særlig eller spesiell kompetanse innen IKT-sikkerhet, særlig innen hendelseshåndtering, for egen sektor
- ha mulighet til å etablere døgnbemanning ved IKT-sikkerhetshendelser, eller på bakgrunn av trusselinformasjon
- ha beredskapsplaner for håndtering av større hendelser, sikkerhetspolitiske kriser og krig knyttet til det digitale rom, avhengig av organisering i sektor
- oppdatere seg gjennom relevante utredninger og årlige og løpende trusselvurderinger rettet mot det digitale rom
- gjennomføre jevnlige risikovurderinger for egen virksomhet rettet mot det digitale rom

NSM skal:

- være det nasjonale fagmiljøet for IKT-sikkerhet
- organisere og drifte Varslingssystem for digital infrastruktur (VDI)
- innhente opplysninger om og holde oversikt over IKT-sikkerhetshendelser og relevante trusler, og opprettholde situasjonsforståelse
- ha oversikt over relevante kompetansemiljøer og ressurser innen IKT-sikkerhet, særlig innen håndtering av IKT-sikkerhetshendelser[17]

[15] Eksempelvis Lysneutvalget (NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*), NSMs årlige *Helhetlig IKT-risikobilde*, NSMs årlige *Risiko*, Etterretningstjenestens årlige *Fokus*, Politiets sikkerhetstjenestes (PST) årlige *Trusselvurdering*, Norsk senter for informasjonssikrings (NorSIS) årlige *Trusler og trender*, KRIPOS årlige *Trendrapport* og temarapporter fra Direktoratet for samfunnssikkerhet og beredskap (DSB) og Forsvarets forskningsinstitutt (FFI).

[16] Se vedlegg: Mal for sambandskatalog og mal for aktørkart.

[17] NSMs kvalitetsordning for bruk av tredjepart innen hendelseshåndtering vil kunne være et viktig hjelpemiddel.

- etablere rutiner for bruk av kryptert kommunikasjon på nasjonalt nivå i håndtering av IKT-sikkerhetshendelser
- kunne sende og motta gradert informasjon på alle graderingsnivåer
- arbeide kontinuerlig for å øke evnen til å avdekke hendelser
- vedlikeholde og utgi et helhetlig risikobilde for det digitale rom, koordinert med partene i FCKS
- informere SRM og virksomheter om sårbarheter
- være en pådriver for opprettelse og videreutvikling av SRM i sektorene
- regelmessig arrangere SRM-forum
- arrangere jevnlige Comcheck-øvelser
- oppdatere SRM om relevante IKT-sikkerhetshendelser og situasjonsbilde
- ha beredskapsplaner for håndtering av større hendelser, sikkerhetspolitiske kriser og væpnet konflikt knyttet til det digitale rom
- oppdatere seg gjennom relevante utredninger og årlige og løpende trusselvurderinger rettet mot det digitale rom
- gjennomføre jevnlige risikovurderinger for egen virksomhet rettet mot det digitale rom

3.2 Deteksjon og vurdering

IKT-sikkerhetshendelser kan oppdages på ulike måter. Det kan være andre lands etterretningstjenester som varsler om en hendelse eller virksomhets IT-avdeling/-partner som oppdager unormal aktivitet på systemene. Det kan også være brukere i en virksomhet som oppdager symptomer på en hendelse, og det kan være virksomhetens samarbeidsparter som oppdager noe unormalt for eksempel gjennom besøk på nettsider eller digital korrespondanse. Videre kan NSM oppdage unormal trafikk på sensorsystemer, eller politiet kan oppdage kriminell aktivitet gjennom etterretning eller etterforskning. De som oppdager at andre er rammet av en IKT-sikkerhetshendelse skal alltid gjøre virksomheten som er rammet oppmerksom på dette.

Når en virksomhet er rammet av en hendelse, gjennomføres det en kartlegging av situasjonen basert på tilgjengelig informasjon. Sentrale spørsmål virksomheten må forsøke å finne svar på er:

- Hvilke systemer er rammet eller står i fare for å bli rammet? Er det noe som tyder på at andre aktører er rammet?
- Hvor kritiske er disse systemene for virksomheten selv og for samfunnet?
- Hvilken informasjon har vi om hva som har skjedd gjennom logger på nettverksaktiviteten og gjennom en sammenstilling av de rapporterte symptomene fra brukere og/eller andre?

SRM skal bistå virksomheten i å analysere informasjonskildene, vurdere alvorlighet og/eller gi tilleggsinformasjon om hendelsen, for eksempel informasjon rapportert fra andre virksomheter i sektor eller fra NSM.

3.2.1 Forventninger til aktørene knyttet til deteksjon og vurdering

Virksomheter forutsettes å:

- ha beredskap for rettidig å avdekke hendelser

- ha kompetanse om relevante systemer i virksomhet og kunne vurdere alvorlighetsgrad, omfang og konsekvenser på overordnet nivå
- kunne vurdere om kritisk infrastruktur og/eller kritiske samfunnsfunksjoner er eller står i fare for å bli berørt av hendelsen
- benytte NSMs system for klassifisering av hendelser, eller et system som er kompatibelt med dette
- vurdere behov for bistand

Sektorvise responsmiljøer skal:

- ha kompetanse om relevante systemer i sektor og kunne vurdere alvorlighetsgrad, omfang og konsekvenser på overordnet nivå
- kunne avgjøre om kritisk infrastruktur og/eller kritiske samfunnsfunksjoner i sektoren er eller står i fare for å bli berørt av hendelsen
- kunne gi råd om videre håndtering og hvem som skal involveres i hendelseshåndteringen
- benytte NSMs system for klassifisering av hendelser

NSM skal:

- ha beredskap for å overvåke VDI
- kunne vurdere om kritisk infrastruktur og/eller kritiske samfunnsfunksjoner er eller står i fare for å bli berørt av hendelsen
- kunne anbefale videre håndtering og hvem som skal involveres i hendelseshåndteringen

3.3 Varsling

Parallelt med den initiale kartleggingen av hendelsen igangsettes varsling. Utgangspunktet for varsling er at den/de som er rammet av en hendelse eier informasjonen om sin hendelse. Det betyr at varsling alltid skal gjøres i overenstemmelse med den/de som eier informasjonen om hendelsen, med mindre lovpålagte forhold tilsier noe annet.[18] Dersom det i en virksomhet finnes konkrete holdepunkter for at andre nære samarbeidspartnere er rammet av samme hendelse, bør det vurderes om disse skal varsles først slik at de kan komme i gang med sin hendelseshåndtering. Dernest må virksomheten vurdere å varsle sitt SRM.

SRM bør alltid varsles dersom virksomheten har betydning for kritisk infrastruktur eller kritiske samfunnsfunksjoner og dersom virksomheten har behov for støtte til å gjenopprette sikker drift, dersom noe tyder på at det kan dreie seg om en avansert hendelse eller en trusselaktør med betydelig kapasitet og/eller det kan antas at hendelsen omfatter flere aktører og eventuelt flere sektorer.

Dersom virksomheten er knyttet til VDI-samarbeidet, har en bilateral avtale med NSM, eller ikke er tilknyttet et SRM, men hendelsen likevel oppfyller kriteriene for å varsle SRM, kan virksomheten kontakte NSM direkte.

[18] Varsling knyttet til konsekvenser av IKT-sikkerhetshendelser gjøres på samme måte som for hendelser i den fysiske verden. Her vil eksterne avtaleparter, politiet og andre beredskapsetater kunne ha viktige roller.

Parallelt med varsling til SRM og NSM skal virksomheten varsle overordnet myndighet i egen sektor, i henhold til sektorens egne prosedyrer og eventuelt politiet.

Når SRM blir varslet om en hendelse eller flere sammenfallende hendelser, varsler SRM videre til NSM og vurderer behov for å varsle andre SRM etter en initial kartlegging av situasjonen. NSM skal i utgangspunktet varsles om alvorlige hendelser som rammer kritisk infrastruktur og kritiske samfunnsfunksjoner. SRM må imidlertid også vurdere å varsle NSM dersom noe tyder på at det kan dreie seg om en avansert hendelse eller en trusselaktør med betydelig kapasitet og/eller det antas at hendelsen omfatter flere sektorer. Dette fordi det da bør kartlegges bredt hvorvidt kritisk infrastruktur og/eller kritiske samfunnsfunksjoner er eller kan komme til å bli berørt.

Parallelt med varsling til andre SRM og/eller NSM varsler SRM overordnet myndighet i egen sektor i henhold til sektorens egne prosedyrer.

NSM varsler andre SRM, VDI-medlemmer og/eller virksomheter NSM har bilaterale avtaler med der det vurderes som relevant. NSM varsler i enkelte tilfeller også andre virksomheter direkte, enten i samråd med SRM eller uten å koordinere med SRM i tilfeller der varsling er tidskritisk.

NSM varsler Felles cyberkoordineringssenter (FCKS) om alvorlige IKT-sikkerhetshendelser som rammer kritisk infrastruktur og kritiske samfunnsfunksjoner.[19]

3.3.1 Forventninger til aktørene knyttet til varsling

Virksomheter forutsettes å:

- ha rutiner for å varsle om IKT-sikkerhetshendelser til SRM og eventuelt samarbeidende virksomheter, samt til NSM under forutsetningene angitt i kap. 3.3

Sektorvise responsmiljøer skal:

- varsle om IKT-sikkerhetshendelser i sektoren til NSM, andre SRM og til relevante virksomheter

NSM skal:

- ivareta rollen som nasjonalt kontaktpunkt for varsling av IKT-sikkerhetshendelser til, og nasjonal varsling om informasjon fra, internasjonale organisasjoner og parter, herunder NATO[20]
- varsle om IKT-sikkerhetshendelser til relevante SRM og virksomheter
- varsle Forsvarsdepartementet og Justis- og beredskapsdepartementet om alvorlige hendelser av nasjonal betydning

[19] Se «*Retningslinjer for cybersamarbeid*» fra 2017.
[20] Norge har to nasjonale kontaktpunkter med NATO, ett nasjonalt (NSM) og ett for militære anliggender (CYFOR/BKI).

3.4 Iverksetting av prosesser og tiltak for å håndtere hendelsen

Hendelseshåndtering kan innebære tiltak for å: 1) stanse hendelsen, begrense skadeomfang og gjenopprette sikker tilstand; 2) sikre tekniske spor og gjøre beslag og/eller pågripelser i forbindelse med etterforskning, og/eller 3) iverksette offensive mottiltak. Rammeverket omfatter imidlertid bare håndtering knyttet til å stanse hendelsen, skadevurdere, begrense skadeomfang og gjenopprette sikker tilstand (jf. definisjon av håndtering av IKT-sikkerhetshendelser, kap 1.1), og nevner bare øvrige tiltak i den grad det er relevant for disse. Tiltak for å begrense skadeomfang og gjenopprette sikker tilstand gjennomføres i hovedsak av virksomheten med eventuell bistand fra eksterne partnere, med støtte fra SRM, NSM og eventuelt politiet.

I mange tilfeller pågår etterforskning samtidig som den tekniske håndteringen for å gjenvinne sikker tilstand pågår. Ved alvorlige hendelser vil det i noen tilfeller kunne oppstå ulike motstridende hensyn samtidig, for eksempel ved at man for å kunne avdekke hvem som står bak en hendelse er nødt til å avvente tiltak for å gjenopprette sikker tilstand. Disse hensynene vil måtte avveies mellom de som er ansvarlige for de ulike tiltakene på nasjonalt nivå.

Tiltak for å gjenopprette sikker tilstand utføres i all hovedsak av virksomheten selv gjennom sin IT-avdeling/-partner. SRM har primært en koordinerende rolle. Dette innebærer informasjonsdeling innad i sektor, på tvers av sektorer og mot NSM. For å kunne drive effektiv informasjonsdeling må SRM etablere og opprettholde et situasjonsbilde i sin sektor. Det forutsettes ikke at SRM skal ha kapasitet til å gjennomføre tiltak direkte på virksomheters systemer.

NSM har en veiledende og koordinerende rolle på teknisk nivå i hendelseshåndteringen. NSM utfører teknisk skadevareanalyse, etablerer et nasjonalt situasjonsbilde i det digitale rom, deler informasjon med SRM og eventuelt virksomheter, etablerer samarbeidsfora for SRM under en pågående hendelse og koordinerer aktiviteten mot politiet, PST og Etterretningstjenesten i samråd med SRM og berørte virksomheter.

3.4.1 Forventninger til aktørene knyttet til iverksetting av prosesser og tiltak for å håndtere hendelsen

Virksomheter forutsettes å:

- etablere, eller ha tilgang til, tilstrekkelig evne og kapasitet til å håndtere IKT-sikkerhetshendelser[21]

Sektorvise responsmiljøer skal:

- ha oversikt over omfang av hendelsen og se hendelser innenfor samme sektor i sammenheng
- gi råd om tiltak til virksomheter innenfor sektoren

NSM skal:

- utlede oppdaterte deteksjonsparametere basert på analyser i håndteringen

[21] Eksempelvis tilgang til tilstrekkelig evne og kapasitet gjennom avtale med kommersiell tredjepart. Se NSMs godkjenningsordning for leverandører som tilbyr tjenester for håndtering av IKT-sikkerhetshendelser.

- gi råd og veiledning til SRM og virksomheter i hendelseshåndteringen
- delta i og lede FCKS
- rådgi Nkom om styring av nettilgang og ressurser, for eksempel gjennom deltagelse i Ekom sikkerhetsforum[22], eller i andre kanaler.
- koordinere hendelseshåndteringen for å gjenopprette sikker tilstand ved alvorlige IKT-sikkerhetshendelser
- anbefale tiltak til politisk ledelse ved alvorlige IKT-sikkerhetshendelser

3.5 Situasjonsrapportering

Under en pågående hendelse er rapporteringslinjene ved håndtering av IKT-sikkerhetshendelser like varslingslinjene slik de er beskrevet over. Situasjonsrapportering skal gå både fra virksomhets- og sektornivå til nasjonalt nivå, og fra nasjonalt nivå til sektor- og virksomhetsnivå.

3.5.1 Forventninger til aktørene knyttet til situasjonsrapportering

Virksomheter forutsettes å:

- benytte NSMs system for rapportering av IKT-sikkerhetshendelser, herunder klassifisering og kategorisering, eller et system som er kompatibelt med dette (vedlegg 4 til rammeverket).
- rapportere alle IKT-sikkerhetshendelser til SRM, også de hendelser som blir håndtert internt i virksomhet. Sistnevnte rapportering kan skje i etterkant av hendelseshåndteringen.

Sektorvise responsmiljøer skal:

- benytte NSMs system for rapportering av IKT-sikkerhetshendelser, herunder klassifisering og kategorisering
- rapportere jevnlig til NSM under en pågående alvorlig IKT-sikkerhetshendelse
- rapportere alle IKT-sikkerhetshendelser til NSM, også de hendelsene som blir håndtert internt i sektor/virksomhet. Sistnevnte rapportering kan skje i etterkant av hendelseshåndteringen.

NSM skal:

- etablere og utvikle en metode for rapportering av IKT-sikkerhetshendelser, herunder klassifisering og kategorisering
- være en pådriver og rådgiver for sektorers anvendelse av ovennevnte metode
- jevnlig rapportere om situasjonsbildet til relevante aktører
- sammenstille og dele relevant informasjon med SRM
- ved direkte samhandling med en virksomhet i en sektor, koordinere dette med aktuell SRM og informere om utviklingen i hendelseshåndteringen[23]
- rapportere til Forsvarsdepartementet og Justis- og beredskapsdepartementet om forhold som påvirker eller kan påvirke stats- og samfunnssikkerhet

[22] Per i dag er dette et møte som arrangeres to ganger per år, men det er planlagt utvidet til å fungere som en møtearena som etableres ved behov i beredskapssammenheng.
[23] Så lenge det ikke strider imot avtaler mellom de involverte partene.

3.6 Tilbakeføring og læring av hendelsen

Etter at hendelseshåndteringen knyttet til å gjenopprette sikker tilstand er avsluttet, starter arbeidet i virksomheten med å lukke sårbarheter og øke grunnsikringen dersom det er nødvendig. Tiltak som iverksettes må baseres på en grundig analyse av hva som gikk galt og om det etablerte sikkerhetsnivået gir god nok sikkerhet.

SRM, kommuner, fylkeskommuner, NSM, DSB, PST og andre arbeider på sektorielt, regionalt og nasjonalt nivå for å analysere sikkerhetstilstanden, lukke sårbarheter og implementere forebyggende sikkerhetstiltak.

3.6.1 Forventninger til aktørene knyttet til tilbakeføring og læring av hendelsen

Virksomheter forutsettes å:

- dersom hendelsen ikke allerede er varslet og/eller anmeldt til politiet, bør dette gjøres av virksomheten
- delta i evalueringsarbeid i egen sektor, avhengig av omfang og involvering
- evaluere og forbedre egen evne til håndtering av IKT-sikkerhetshendelser
- implementere tiltak for å styrke evne til å motstå lignende hendelser senere (grunnsikring)
- dele læringspunkter etter en hendelse med SRM

Sektorvise responsmiljøer skal:

- delta i evalueringsarbeid sammen med NSM
- støtte virksomheter i egen sektor ved evaluering av hendelser
- evaluere og forbedre egen evne til å utføre aktivitetene innenfor håndtering av IKT-sikkerhetshendelser som er innenfor SRMs ansvarsområde
- implementere tiltak for å øke evnen til å utføre aktivitetene innenfor håndtering av IKT-sikkerhetshendelser som er innenfor SRMs ansvarsområde ved liknende hendelser senere
- gi råd til virksomheter om tiltak for å bedre grunnsikring
- dele læringspunkter etter en hendelse med virksomheter i sektor og NSM

NSM skal:

- oppdatere VDI med signaturer fra håndteringen for å øke sannsynligheten for at fremtidige sikkerhetshendelser av samme karakter detekteres
- utarbeide rapport etter alvorlige hendelser som er håndtert i samarbeid med SRM og involverte virksomheter
- dele læringspunkter etter alvorlige hendelser med SRM
- dele læringspunkter etter alvorlige hendelser med relevante myndigheter for å sikre at krav og anbefalinger er mest mulig hensiktsmessige og målrettede med hensyn til risikobildet
- evaluere og forbedre egen evne til håndtering av IKT-sikkerhetshendelser
- implementere tiltak for å øke evnen til å håndtere liknende hendelser senere
- gi råd til virksomheter og SRM om tiltak for å bedre grunnsikring og øke håndteringsevnen

4 Vedlegg til rammeverket

Rammeverkets vedlegg revideres som hovedregel samtidig med hoveddokumentet, men kan revideres utenom dette ved behov. Revisjoner av vedleggene gjennomføres og godkjennes av NSM.

Nr.	Navn	Merknad
1	Prinsippskisse	
2	Mal for aktørkart	Aktørkart innhentes av SRM fra virksomheter i sektor. SRM sammenstiller aktørkart for sektor og oversender dette til NSM. **Merk at aktørkart kan være sikkerhetsgradert informasjon. Særlig gjelder dette aktørkart som er sammenstilt for flere virksomheter eller hele sektor. Det er den som produserer og/eller sammenstiller informasjonen som foretar verdivurdering og fastsetter gradering.**
3	Mal for sambandskatalog	Sambandskatalog innhentes av SRM fra virksomheter i sektor. SRM sammenstiller sambandskatalog for sektor og oversender dette til NSM. **Merk at sambandskatalog kan være sikkerhetsgradert informasjon. Særlig gjelder dette sambandskataloger som er sammenstilt for flere virksomheter eller hele sektor. Det er den som produserer og/eller sammenstiller informasjonen som foretar verdivurdering og fastsetter gradering.**
4	Begrepsliste	
5	Klassifisering av IKT-sikkerhetshendelser	Et rapporteringsformat for IKT-sikkerhetshendelser, der klassifisering av IKT-sikkerhetshendelser er ett element, er under utarbeidelse. Arbeidet ledes av NSM i samarbeid med SRM. Dette vedlegget erstattes av vedlegget «Rapportering av IKT-sikkerhetshendelser» når dette er ferdigstilt.