Rapport

Avdekke, håndtere og etterforske digitale angrep

For Lysneutvalget

20.03.2015

mnemonic
- securing your business

Innledning

Lysneutvalget etablerte i januar 2015 en ressursgruppe med den hensikt å få innspill fra operative miljøer i Norge involvert i arbeid med avdekking, håndtering og etterforskning av digitale angrep. Ressursgruppa møttes tre ganger i perioden januar-februar 2015, og med bakgrunn i disse møtene ble denne rapporten utarbeidet.

«Digitale angrep» er et er begrep som kan ha ulik betydning, avhengig av hvem vi spør. Ressursgruppa har ikke gjort noe forsøk på å definere begrepet, men har diskutert ulike situasjoner som kan falle inn under begrepet, slik som sabotasje av infrastruktur eller programvare gjennom fiendtlig tilgang til systemer, spionasje fra statlige og ikke-statlige aktører i informasjonssystemer og datanettverk og kampanjer med økonomiske motiver som treffer norske nettverk i stor grad. Dette har dannet grunnlaget for de videre diskusjonene og vurderingene av Norges evne til å avdekke, håndtere og etterforske digitale angrep.

Rapporten inneholder en beskrivelse av nå-situasjon, utfordringer ressursgruppa ser innenfor dagens situasjon og forslag til tiltak. Ressursgruppa har bestått av representanter fra ulike organisasjoner, og som rapporten beskriver har det ikke vært enighet rundt alle temaer som har vært diskutert. De operative miljøene er imidlertid enige om at det er behov for mer målrettet arbeid og samarbeid rundt å avdekke, håndtere og etterforske digitale angrep.

Lysneutvalget står videre fritt i hvordan de ønsker å innholdet i denne rapporten i sitt videre arbeid, men vi håper selvsagt at innspillene vil komme til nytte. Ressursgruppa ønsker Lysneutvalget lykke til, og ser fram til å lese den endelige NOUen når den foreligger.

Innholdsfortegnelse

1 Oppdraget

1.1 Oppdragsbeskrivelse

Oppdraget som ble gitt fra Lysneutvalget er som følger:

Oppdraget er å beskrive dagens kapabilitet for både næringslivet og samfunnsviktige virksomheter når det gjelder å kunne avdekke (proaktivt og reaktivt), håndtere (inkludert koordinere, lede, avgrense) og etterforske (både privat- og politietterforskning) digitale angrep. Lysneutvalget skal selv beskrive aktørenes rolle og ansvar, men i den grad det avdekkes uklare roller- og ansvarsfordeling mellom aktørene, er dette viktig å vise til. Arbeidet skal ikke behandle generelle forebyggende tiltak.

Arbeidet skal omfatte en **gap-analyse** med følgende vurderinger med hensyn til kombinasjonen av det private og offentliges evne til å avdekke, håndtere og etterforske digitale angrep i forhold til:

- Effektivitet
- Kapasitet
- Informasjonsinnhenting og -deling (nasjonal og internasjonalt) av relevant informasjon, herunder praksis for håndtering av vern om personopplysninger
- Analysekapabilitet
- Samarbeid (privat-offentlige og eventuelt sivil-militært)
- Generell evne til å bistå i andre enheter (privat og offentlig) og
- Evne til læring og evaluering av hendelser og øvelser for å forbedre kapabilitet.

I tillegg til gap-analysen skal det foreslås overordnede tiltak for å lukke disse. De anbefalte tiltakene kan være av **regulatorisk, strukturell, organisatorisk, teknologisk eller kompetansemessig** karakter.

1.2 Begrensninger

Ressursgruppa er satt sammen ved at Lysneutvalget har forespurt virksomheter og representanter fra disse om deltakelse. Virksomhetene som er representert har stort fokus på arbeid med ulike former for digitalt angrep, og representantene i gruppa har mye erfaring. De har også relativt ulik bakgrunn, og rapporten reflekterer at det ikke har vært enighet om alle temaer som har vært diskutert. Det er mange hensyn som skal balanseres når det gjelder arbeid med digitale angrep.

Rapporten er ført i pennen av mnemonic. Der mnemonic har supplert med tilleggsinformasjon eller vurderinger utover det som er diskutert av ressursgruppas medlemmer, er dette beskrevet i teksten.

Informasjonsinnhentingen til rapporten er gjennomført i en kort periode fra starten av januar til midten av februar 2015. Arbeidet ble dermed intensivt, og tiltakene kunne vært detaljert i større grad med noe mer tid til refleksjon og diskusjon.

Etterretningstjenestens representant understreker at det er sikkerhetsgraderte sider ved sakskomplekset som ikke kan belyses i rapporten. Dette påvirker analyser og konklusjoner relatert til tiltak mot de mest alvorlig og avanserte trusler i det digitale rom.

Det er også viktig å poengtere at medlemmene i ressursgruppa har representert sine respektive organisasjoner. Enkelte av diskusjonene i gruppa har vært av en slik art at det ikke har vært naturlig for alle representantene å delta.

Ressursgruppa har videre ikke hatt representanter fra påtalemakten og det var heller ikke en del av oppdraget som ble gitt fra Lysneutvalget.

1.3 Forkortelser brukt i rapporten

CSIRT: Computer security incident response team.

CERT: Brukes i mange tilfeller synonymt med CSIRT.

CKG (cyberkoordineringsgruppen): Består av NSM NorCERT, Politiets sikkerhetstjeneste og Etterretningstjenesten

Utvidet CKG: Består i tillegg til CKG av Kripos og Cyberforsvaret

2 Beskrivelse av nå-situasjon og gapanalyse

2.1 Hva er et «digitalt angrep»?

Et av problemene vi ofte støter på i arbeid med informasjonssikkerhet og hendelser relatert til dette, er at det brukes ulike begreper og det legges ulik betydning i samme begrep avhengig av hvilken bakgrunn vi har. Både «digitalt angrep», «hendelse», «IKT-kriminalitet» og «cyberangrep[1]» er eksempler på dette. Et problem med disse betegnelsene er at de potensielt skjuler situasjoner av svært ulik karakter. Ved å benevne dem med en kategori vi ikke definerer godt nok, blir det vanskelig å adressere nødvendige problemstillinger på en tilfredsstillende måte.

Innenfor begrepet «digitale angrep» har ressursgruppa diskutert situasjoner som:

- Sabotasje av infrastruktur eller programvare gjennom fiendtlig tilgang til systemer
- Spionasje fra statlige og ikke-statlige aktører i informasjonssystemer og datanettverk
- Kampanjer med økonomiske motiver som treffer norske nettverk i stor grad, for eksempel banktrojanere mot norske nettbanker.

Grensene mellom ulike situasjoner, begreper og teknikker er ikke nødvendigvis enkle å trekke opp. Intensjon ble i gruppa trukket fram som et vesentlig element i forståelsen av begrepet «digitalt angrep». En situasjon i den digitale verden som har oppstått fordi en trusselaktør har hatt en intensjon om å ramme norske interesser økonomisk, politisk eller samfunnsmessig, vil således kunne inngå i begrepet «digitalt angrep».

Videre har gruppa diskutert at det er viktig at også situasjoner som blir håndtert før de får konsekvenser av betydning, kan regnes som «digitalt angrep». Et eksempel på det er der det er bygd opp gode sikkerhetsmekanismer som stanser et distribuert tjenestenektangrep.

Det har også vært diskutert hvorvidt for eksempel ID-tyveri skal inkluderes i forståelsen av begrepet digitalt angrep. Representanter i ressursgruppa mener at noe av problemet med diskusjonen nettopp er at ID-tyveri da havner i samme kategori som sabotasje av kritisk infrastruktur, og selv om det er vesentlig for de som rammes, har vi valgt å ikke inkludere det i begrepet i denne rapporten.

Det er verdt å merke seg at særlig for representanter med forsvarsbakgrunn i gruppa, er begrepet «angrep» snevrere enn de situasjonene beskrevet ovenfor. En parallell til begrepet «digitalt angrep» kan vi imidlertid finne i Forsvarsdepartementets cyberretningslinjer, men her benevnt ved «cyberangrep». Nettverksoperasjoner er begrepet som brukes av NSM NorCERT, Politiets sikkerhetstjeneste og Etterretningstjenesten på i hvert fall deler av det som her forstås med digitale angrep.

Vi vil videre i rapporten bruke begrepet «digitale angrep», med mindre det er behov for å være mer presise på hva slags situasjon vi beskriver.

2.2 Aktører

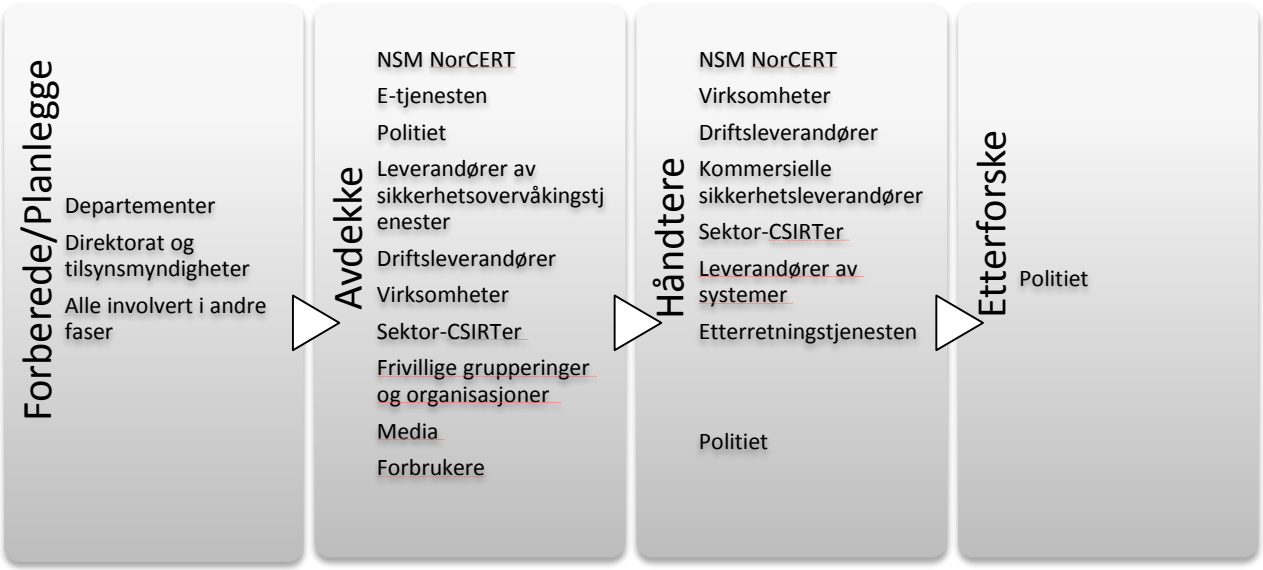
Det er mange som i dag har roller innenfor operativt å avdekke, håndtere og etterforske digitale angrep, som beskrevet i Figur 1. For å være mer spesifikke, må vi igjen se på hvilke former for digitale

[1] https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf

angrep vi snakker om, ettersom ulike aktører vil være involvert i ulike saker. Det kan i tillegg være ulik oppfatning av hva som inngår i de ulike begrepene avdekke, håndtere og etterforske. Vi har også inkludert forberede og planlegge.

I denne rapporten har vi lagt følgende i de ulike begrepene:

Begrep/fase	Forklaring
Forebygge/planlegge	Aktiviteter for å planlegge og forberede hvordan vi gjør arbeidet i de andre fasene.
Avdekke	Aktiviteter for å oppdage digitale angrep eller forsøk på det.
Håndtere	- Aktiviteter for å redusere omfang og konsekvens av digitalt angrep, enten for den enkelte virksomhet som er rammet eller for samfunnet som helhet. - Operativ håndtering (for eksempel lede og koordinere samfunnsressursene) av politiet i forbindelse med alvorlig digitale angrep med samfunnsmessige konsekvenser.
Etterforske	Etterforskning utført av politiet



Figur 1 Operative aktører involvert i arbeidet med "digitale angrep".

2.3 Forberede og planlegge

For å arbeide godt med å avdekke, håndtere og etterforske digitale angrep, er det en del mekanismer som må være på plass. Det må være tydelig definert hvem som har roller og ansvar i forbindelse med arbeidet, myndighet må følge ansvaret og det bør etableres en plan for hvordan det skal arbeides med ulike typer digitale angrep. Dette handler i praksis om å etablere en plan for å arbeide med digitale angrep (incident response plan).

Myndighetenes ambisjonsnivå

Fra myndighetsnivå er det ulike departementer, direktorater og tilsynsmyndigheter som er involvert i å sette krav og betingelser for avdekking, håndtering og etterforsking av digitale angrep. Ressursgruppas medlemmer etterspør et tydeligere ambisjonsnivå fra myndighetene når det gjelder disse temaene. Det er noe uklart for ressursgruppa hvorvidt utydeligheten kommer fra departementsnivå eller lenger nede i hierarkiet. Resultatet er imidlertid at andre aktører (virksomheter og leverandører) ikke vet konkret hva de har å forholde seg til fra myndighetenes side. Det kan både føre til at det etableres miljøer i parallell som håndterer samme problemstillinger (for eksempel analysemiljøer), men også at oppgaver ikke blir løst, fordi det ikke er tydelig hvor ansvaret ligger.

Det er også en oppfatning i ressursgruppa at bevilgninger og tiltak som iverksettes ikke alltid er de mest effektive for å bedre den faktiske evnen til å avdekke, håndtere og etterforske digitale angrep. Hvorvidt årsaken til dette ligger på bestiller-siden eller hos de som implementerer og iverksetter tiltakene, har ikke ressursgruppa tilstrekkelig med informasjon til å vurdere.

Det er nyanser innenfor dette området, der noen funksjoner har klarere roller og ansvar enn andre. Hovedinntrykket er uansett at det er uklart, og da særlig mellom ulike funksjoner.

Beslutningsmyndighet

I forbindelse med arbeid med digitale angrep, vil det være behov for å ta flere større og mindre beslutninger. Nasjonalt opplever ressursgruppa at det ikke entydig hvem som har beslutningsmyndighet til for eksempel å iverksette tiltak som har motstridende interesser for den virksomheten eller sektoren som er rammet og NSM NorCERT. Dette kommer for eksempel til uttrykk i forholdet mellom sterke sektormyndigheter og myndigheter med særlig ansvar for sikkerhet. Der virksomheter er underlagt andre tilsynsmyndigheter, kan koblingen mellom NSM og NSM NorCERT komplisere bildet for virksomheten som er rammet av hendelsen.

I flertallet av hendelser som håndteres ligger det meste av beslutningsmyndighet i praksis hos de ulike virksomhetene som rammes. NSM NorCERT peker på at de er inne og bistår med håndtering av alvorlige dataangrep, men har ingen myndighet til å pålegge virksomheter å utføre arbeid, utlevere data eller la systemer stå i drift til støtte for kartleggingsformål. Politiet har dette i dag i noen grad gjennom hjemler i politiloven m.fl., men er i mindre grad involvert i operativ håndtering av digitale angrep.

Hvis vi ser på alvorlige digitale angrep hvor intensjonen til trusselaktøren er å skape fysisk skade, havner vi raskt inn i en beredskapssituasjon hvor tradisjonelle beredskapsmyndigheter og prinsipper trer inn. Dette er type situasjoner vi har liten erfaring med i praksis, men som gjerne brukes som grunnlag i øvelser.

Utstrakt kunnskap om trusselbildet

Ressursgruppa har også diskutert viktigheten av at beslutningstakere på alle nivåer har tilstrekkelig informasjon om trusselbildet, slik at de kan ta begrunnede beslutninger. Politiets sikkerhetstjeneste gjør en viktig jobb med å informere ledelsen i ulike virksomheter om trusselbildet. Dette er imidlertid informasjon som ikke alltid tilfaller alle beslutningstakere i virksomheten, noe som igjen kan føre til at det tas beslutninger som med utilstrekkelig informasjon. Videre er det begrensninger i hvor mange virksomheter Politiets sikkerhetstjeneste kan informere om detaljer i trusselbildet. Selv om de mest samfunnskritiske virksomhetene blir informert, er ressursgruppa bekymret for den helhetlige forståelsen av trusselbildet.

Virksomhetenes og statens ansvar

Ressursgruppa mener at det er et viktig prinsipp at de enkelte virksomheter har et selvstendig ansvar for å sørge for beskyttelse mot og evne til å håndtere digitale angrep. Hvor langt dette ansvaret strekker seg, er det imidlertid ikke full konsensus om i gruppa. At virksomhetene har et selvstendig ansvar for å forstå sine egne informasjonssystemer og gjøre kosteffektive tiltak som kan redusere sårbarheter og gjøre det mulig å framskaffe informasjon om og logger fra sine systemer, støttes gjennomgående av gruppa. Det pekes videre på at virksomheter kan være villige til å ta risiko som ikke er akseptabel i et nasjonalt perspektiv. En forutsetning for at en overordnet nasjonal mekanisme skal fungere, er at det finnes tydelige retningslinjer for hvordan dette skal håndteres.

Krav gjennom lover, forskrifter og tilhørende tilsyn

Myndighetene gjennom ulike direktorat og tilsynsmyndigheter har en viktig rolle når det gjelder å stille krav til virksomheter innenfor sin sektor. Det er slik ressursgruppa oppfatter det i dag liten grad av samordning på tvers av ulike kravstillere. Enkelte myndigheter stiller svært detaljerte krav, mens andre stiller svært åpne krav. Ressursgruppa peker også på områder hvor krav til logging og sletting av samme form for informasjon underlegges ulike krav i ulike lovverk (for eksempel kan informasjon relatert til bokføring som i henhold til regnskapslovgivning skal oppbevares i 10 år i enkelte virksomheter, være samme type informasjon som av personvernhensyn i andre virksomheter skal slettes innen 21 dager).

Ressursgruppa har også diskutert relevansen av en del lover, forskrifter og tilhørende tilsyn når det kommer til å øke den faktiske sikkerheten og legge til rette for praktisk å avdekke, håndtere og etterforske digitale angrep. I enkelte tilfeller oppleves regelverket så fjernt fra det som anses som relevante og effektive tiltak for å øke sikkerhet, at virksomhetene gjennomfører compliance-aktiviteter (oppfyllelse av lover og regler) mer eller mindre frikoblet fra det operative arbeidet med sikkerhet.

Øvelser

Det er potensielt mange offentlige og private aktører involvert i hendelser og øvelser, og samhandling blir en vesentlig del av god deteksjon og håndtering. Store øvelser i regi av myndighetene har som ambisjon å øve på koordinering og varsling, gjerne mellom sektorer. Ressursgruppa mener som beskrevet over at myndighet, ansvar og rollefordeling i for liten grad er planlagt, bestemt og kommunisert, og øvingen blir derfor lite hensiktsmessig. Tiltak som identifiseres gjennom øvelsene, blir videre i liten grad implementert, ettersom det ikke finnes prosesser og prosedyrer å implementere tiltakene i, og ansvaret for implementeringen blir uklart.

Flere av de sektorvise responsmiljøene som etableres, for eksempel FinansCERT og KraftCERT, har øvelser for medlemmene som en del av sin tjenesteportefølje.

Evaluering av hendelser

I forbindelse med større hendelser som involverer flere aktører, er det fokus på evaluering i etterkant av hendelser. Det virker imidlertid som det er en tendens til at nye hendelser prioriteres over evaluering av allerede håndterte hendelser. Det kan både bety at det ikke gjennomføres noen grundig evaluering i etterkant, eller at tiltak som identifiseres ikke blir implementert.

Drifts- og tjenesteleverandører

For å kunne avdekke og håndtere digitale angrep hvor drifts- og tjenesteleverandører er en del av kjeden kreves det effektivt samarbeid. Ressursgruppa peker spesielt på rapportering om mistanke om angrep, verktøy og prosesser for innhenting av informasjon og effektiv kommunikasjon mellom leverandør(er) og kunde som vesentlig. Ressursgruppen ser at dette er vanskelig å løse gjennom hver enkelt virksomhets avtale med leverandøren, og det krever en del fra leverandører å få dette til. Ved at alle kunder har ulike krav i kontraktene oppstår det problemer for leverandørene i å møte dem.

Det er også viktig å løfte sikkerhet og kvalitet i anskaffelsesprosesser. Dette vil i de aller fleste tilfeller øke kostnaden, og dersom pris er det viktigste kriteriet, taper gjerne leverandørene med sikkerhet og kvalitet innebygd i leveransene. Det kan også være at leverandører (og kunder direkte) velger å sette ut deler av en leveranse til lavkostland for å redusere kostnader. Det kan ha konsekvenser for eksempel for uthenting av data, fordi vi ikke kan styre andre land gjennom lovgivning.

Samarbeid med Forsvaret

Forsvaret (utenom Etterretningstjenesten) har i dag et begrenset samarbeid med det sivile samfunnet innenfor temaet digitale angrep. Det er unntak, der private virksomheter for eksempel samarbeider med Cyberforsvaret om kurs og øvelser, men det er begrenset til et lite antall virksomheter. I forbindelse med håndtering av alvorlige digitale angrep har øvelser som Cyberdawn vist at prosessen med bistandsanmodninger tar lang tid, og at det ikke fungerer hensiktsmessig for disse problemstillingene.

Statistikk

Det finnes ingen helhetlig statistikk over omfanget av digitale angrep i Norge. Aktører involvert i å avdekke, håndtere og etterforske digitale angrep, holder statistikk over saker de er involvert i, men dette samles ikke noe sted. Enkelte sektorer stiller krav om rapportering av hendelser, men det er ingen entydig kategorisering eller samling heller av denne typen rapporter.

Oppsummering av 2.3

Gap	Tiltak
Det er behov for en tydeligere implementert plan for arbeid med digitale angrep enn det vi har i dag, inkludert roller, ansvar og myndighet mellom ulike aktører.	3.1.1 Ambisjonsnivå 3.1.2 En plan for håndtering av digitale angrep

	3.1.3 Prinsipielt skille på tilsyn og operative enheter
Øvelsene som gjennomføres fra myndighetene i dag, er gjerne veldig store og har som ambisjon å sjekke ansvar og myndighet mellom ulike funksjoner. Effekten av øvelsene er for de virksomhetene som deltar i beste fall varierende.	3.4.5 Gjennomføring av øvelser
Ikke alle relevante beslutningtakere i viktige virksomheter sitter med tilstrekkelig informasjon om trusselbildet til å gjøre riktige beslutninger.	Utover videre informasjonsarbeid fra relevante myndigheter og oppfordring til virksomheter som utsettes for digitale angrep om å være åpne om det, har ikke ressursgruppa diskutert noen konkrete tiltak på dette området.
Det er noe mangler i evaluering i etterkant av større digitale angrep på tvers av virksomheter og funksjoner.	3.4.6 Læring etter hendelser
Drifts- og tjenesteleverandører er i stor grad involvert i leveranser til norske virksomheter, men kravene til avdekking og håndtering av digitale angrep er enten sprikende eller ikke-eksisterende.	3.5.8 Lovmessige krav til leverandører 3.5.9 Sertifisering av leverandører
Ikke alle lover og regler oppleves av ressursgruppa som like oppdaterte og hensiktsmessige til bruk innenfor digitale angrep. Dagens straffebestemmelser er ikke laget med tanke for det digitale rom.	3.5.3 Oppdatering av lover og regler
For store avstander mellom regelverk mellom ulike sektorer når det gjelder arbeid med digitale angrep.	3.5.4 Felles basis for regelverk på tvers av bransjer
Forsvaret (utenom Etterretningstjenesten) har i dag et begrenset samarbeid med det sivile samfunnet innenfor arbeid med temaet digitale angrep	3.5.7 Enklere bistandsanmodninger?
Det finnes ingen helhetlig statistikk over omfanget av digitale angrep i Norge i dag.	3.5.2 Rapportering av hendelser

2.4 Avdekke

Deteksjonsmekanismer

For effektiv avdekking av digitale angrep, trengs det gode deteksjonsmekanismer som dekker de kanaler hvor angrepene gjennomføres. Dagens deteksjonsmekanismer er i stor grad basert på signaturer, som krever at angrepet må være kjent før det kan oppdages. Det finnes også mekanismer som baserer seg på å analysere oppførsel i systemene, og varsle om unormal oppførsel. Dette er i de fleste tilfeller mer avansert, og gjøres i mindre grad. Trusselaktørene krypterer videre trafikken sin i økende grad, noe som er en stor utfordring for nettverksbaserte deteksjonsmekanismer. Vi ser også økende grad av kryptering av regulær Internettrafikk, der ulike kilder rapporterer ulike tall, men et snitt på verdensbasis i dag ser ut til å ligge på ca 20%[2].

Det er også viktig å jobbe koordinert med deteksjon, slik at de ressursene vi har brukes mest mulig effektivt. NSM NorCERTs representant i ressursgruppa mener at ingen klarer dette alene, og at vi er avhengige av at norske myndigheter bidrar. Det er også urealistisk å tro at vi vil lykkes med å avdekke alt. Etterretningstjenestens representant i gruppa mener like fullt at man bør ha som ambisjon å avdekke de mest alvorlige digitale angrep, hvilket krever tiltak og samvirke utover dagens organisering og kapasiteter.

NSM NorCERTs sensornettverk

NSM NorCERT har bygd opp et sensornettverk (VDI), hvor målet er å ha sensorer for deteksjon av digitale angrep hos et representativt utvalg virksomheter med kritisk infrastruktur og informasjon. Hovedhensikten med sensorene er å avdekke og kartlegge alvorlige digitale angrep mot et representativt utvalg av norske virksomheter. Dette gir grunnlag for et oppdatert digitalt risikobilde. I tillegg varsler NSM NorCERT virksomhetene dersom de oppdager forhold som bør undersøkes videre. VDI-sensornettet har et signatursett som er utviklet basert på tidligere hendelser og annen kjent aktørinformasjon og er videre tilpasset oppgaven med å gi oversikt over det digitale risikobildet mot kritisk infrastruktur. Det er ikke innrettet for deteksjon av de mest alvorlige og ukjente digitale trusler. Det er ingen krav til noen spesielle virksomheter om å delta i VDI-samarbeidet, og de private som deltar må betale en avgift. VDI-sensorene har begrenset mulighet til å se innholdet i trafikk som går kryptert. Det finnes både graderte og ugraderte sensorer.

VDI-sensorene gir NSM NorCERT viktig informasjon. Det er imidlertid viktig å påpeke at både andelen virksomheter som inngår i nettverket og begrensninger i teknologien, gjør at VDI-sensornettverket etter ressursgruppas mening ikke dekker behovet for å avdekke digitale angrep mot kritisk infrastruktur og informasjon i Norge i dag.

Overvåking utover VDI

En del virksomheter gjør overvåking av interne nett og systemer, enten selv (et relativt lite antall) eller gjennom leverandører av denne typen tjenester. Både NSM NorCERTs operasjonssenter og leverandører av denne type tjenester driver overvåking 24/7. Større linje- og driftsleverandører i Norge har de siste årene etablert mekanismer for å tidlig avdekke og stanse distribuerte tjenestenektangrep. Vi ser også en tendens til tettere samarbeid mellom driftsleverandører og leverandører spesialisert på IT-sikkerhet rundt for eksempel sikkerhetsovervåking og logganalyse.

[2] (mnemonic AS, 2015)

Det er store forskjeller når det gjelder grad av overvåking i ulike virksomheter og bransjer. Disse forskjellene kan ha ulike årsaker. Vi ser at virksomheter som har vært rammet av alvorlige digitale angrep i større grad har systemer på plass for å avdekke og undersøke nye forsøk. Dette ser vi for eksempel tydelig i selskaper som har vært utsatt for målrettede spionasjeangrep. Disse vil i større grad ha etablert deteksjonsmekanismer som avdekker ukjente angrep, i tillegg til mer tradisjonelle signaturbaserte systemer.

Det er også forskjell på ulike typer nett og systemer, særlig det vi kaller kontornett og prosessnett. I prosessnett finner vi IKT-systemer som styrer fysiske prosesser. Disse nettene har tradisjonelt vært isolert, og i liten grad vært utsatt for digitale angrep. Etter hvert blir disse i større og større grad koblet sammen med andre nett. Selv om vi både kjenner til virksomheter som gjør overvåking i prosessnett, og det er ulike prosjekter nasjonalt og internasjonalt som jobber med det, er ressursgruppas oppfatning at modenhet rundt deteksjon av digitale angrep i disse nettene generelt er lav.

Virksomheter med ledere og nøkkelpersoner som forstår trusselbildet og behovet for overvåking, vil i større grad prioritere gode mekanismer for å avdekke digitale angrep, slik at det også delvis blir personavhengig. I tillegg ser det ut til at størrelsen på virksomheten vil ha betydning for evnen til å avdekke digitale angrep. Mindre virksomheter kjøper overvåkingstjenester i mindre grad enn større, og har som regel mindre intern kompetanse på området.

Det er viktig å understreke at temaene i dette avsnittet presenterer generelle trekk, og vi kan ikke kun på bakgrunn av for eksempel størrelse og bransje sikkert fastslå virksomhetens modenhetsnivå innenfor arbeid med digitale angrep.

Informasjonsdeling

Effektivitet innenfor området «avdekke digitale angrep», henger sammen med at vi har god og effektiv informasjonsdeling. Dette omfatter sensorer ved kritiske virksomheter og samfunnsfunksjoner, systemer til å raskt omsette deteksjon til varsel, samt kontinuerlig oppdatering av nødvendig kunnskap, etterretning og regelsett til å avdekke de prioriterte truslene.

Oppsummering av 2.4

Gap	Tiltak
Dagens deteksjonsmekanismer er ikke tilstrekkelige for å oppdage alvorlige digitale angrep. Årsaken er både omfang/utbredelse og funksjonalitet.	3.3.1 Deteksjonsmekanismer 3.3.2 Automatisert deling av indikatorer
I mange virksomheter er det manglende kompetanse og prioritering innenfor dette feltet.	3.4.4 Kompetanse i virksomhetene
Avdekking av digitale angrep er i liten grad del av drifts- og tjenesteleverandørers leveranser.	3.5.8 Lovmessige krav til leverandører 3.5.9 Sertifisering av leverandører

2.5 Håndtere

Effektiv håndtering av digitale angrep krever klare roller, ansvar og mandater.

NSM NorCERTs rolle

Sjef NSM er, ifølge Forsvarsdepartementets instruks av 5/12-14, pkt 12, «ansvarlig for å koordinere håndteringen av alvorlige IKT-angrep mot samfunnskritisk infrastruktur eller andre viktige samfunnsfunksjoner». I følge NSMs hjemmesider har NSM NorCERT i dag som viktig oppgave å «håndtere alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon[3]».

Når saker meldes inn til NSM NorCERT, gjøres det en vurdering og prioritering i operasjonssenteret. Enkelte saker diskuteres også i cyberkoordineringsgruppa (CKG), før NSM NorCERT bestemmer om de skal bistå i håndteringen av saken eller ikke. CKG legger ikke føringer på NSM NorCERT sine prioriteringer, men diskusjonene kan gi et bredere bilde av trusselen. Det gjøres også en fordeling av ansvar for saker der det er behov for det. De viktigste kriteriene for prioritering er potensielle konsekvenser og omfang ved hendelsen. I tillegg vil saker som gir stort potensiale for å heve myndighetenes, sektorens eller samfunnets forståelse for IKT-trusselbildet kunne prioriteres. Riktige prioriteringer forutsetter at NSM NorCERTs operatører har god forståelse av ulike virksomheters funksjon, og kan gjøre vurderinger basert på hvilke verdier de ulike virksomhetene forvalter. Medlemmer i ressursgruppa kan vise til saker hvor de har bedt om bistand fra NSM NorCERT til det de mener er alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon uten å bli prioritert. Måten saker prioriteres på kan oppfattes som uforutsigbart for virksomhetene som blir utsatt for digitale angrep. Det er også en utfordring for kommersielle leverandører å vite hvilke tjenester de skal tilby i dette bildet.

NSM NorCERT kan bistå med både koordinering av hendelser og teknisk analyse av maskiner, skadelig kode og logger. De gjør også informasjonsinnsamling gjennom nettverket sitt av andre nasjonale responsmiljøer og CKG med samarbeidspartnere.

Andre nasjonale CSIRT-miljøer

Større selskaper velger å bygge opp egne miljøer, enten internt i virksomheten, gjennom sektorvise responsmiljøer, eller også begge deler som er tilfellet for eksempel for DNB. Det fører til mindre miljøer som gjør parallelle aktiviteter, og det er vanskeligere å tiltrekke seg og beholde personer med tilstrekkelig kompetanse ettersom tilfanget av spennende arbeidsoppgaver blir mindre. Dette gjør den totale utnyttelsen av ressursene i Norge med kompetanse innenfor digitale angrep mindre effektiv.

Det er etablert ulike sektorvise responsmiljøer, for eksempel i finans-, helse- og justissektoren. Dette er delvis som svar på behov i de ulike sektorene som ikke dekkes av NSM NorCERT og delvis som svar på handlingsplanen for nasjonal strategi for informasjonssikkerhet. Disse sektorvise responsmiljøene er svært ulike, noe som kan medføre at samarbeid og koordinering mellom disse fungerer mindre hensiktsmessig. Det er også en utfordring at sektor-CSIRTene ikke nødvendigvis favner hele sektoren. En tredje utfordring med framgangsmåten med sektorvise responsmiljøer er at det ikke er alle virksomheter som har en sterk og naturlig tilhørighet i en sektor. En av

[3] http://nsm.stat.no/tjenester/handtering/

ressursgruppas medlemmer utalte at «trusselaktørene på Internett tar ikke hensyn til at Norge er delt inn i ulike sektorer». NSM NorCERT arrangerer forum for sektor-CSIRTene, men det virker ikke å være noe tett samarbeid mellom disse. Det betyr at informasjonen sektor-CSIRT har ervervet seg som kan være av interesse for andre miljøer ikke deles med andre sektor-CSIRT gjennom standard prosesser og grensesnitt, men at delingen i for stor grad blir personavhengig og tilfeldig.

Cyberforsvaret har en organisert og utrustet operativ avdeling klare til utrykning. Å utnytte denne for den sivile delen av samfunnet krever imidlertid en bistandsanmodning, som erfaring fra øvelser viser at det tar tid å få igjennom.

Drifts- og tjenesteleverandører

De fleste virksomheter i Norge benytter drifts- og tjenesteleveranser i større og mindre grad. Dette kan ha konsekvenser for effektiviteten i forbindelse med håndtering av hendelser. Noen leverandører har i for liten grad skilt ulike kunder, slik at for eksempel iverksettelse av tiltak for effektivt å hindre spredning av skadelig kode kan være vanskelig uten å påvirke driften til andre kunder. Dersom tjenestene leveres fra andre land, og kunden ikke har stilt tilstrekkelig presise krav til overlevering av data i forbindelse med håndtering av digitale angrep, må gjerne de nasjonale CSIRT-funksjonene involveres, og informasjonen må gjennom mange ledd før den når de operative miljøene som faktisk kan nyttiggjøre seg den. mnemonic har også eksempler fra nylige hendelser på at data ikke har blitt overlevert på grunn av den politiske situasjonen mellom Norge og det aktuelle landet. Dette kan føre til betydelige forsinkelser for håndtering av alvorlige dataangrep.

Politiets rolle

Når det gjelder politiets rolle i forbindelse med håndtering av digitale angrep, må vi være tydelige på hva vi legger i begrepet håndtering. Teknisk håndtering for å begrense omfang eller konsekvenser for den enkelte virksomhet er i utgangspunktet virksomhetens ansvar. Politiets operative rolle kommer til uttrykk når hendelser pågår, eksempelvis i et terrorangrep. Den operative utelederen fra politiet tar da beslutninger og leder/koordinerer ressursinnsatsen på stedet, og ved større hendelser settes det ned stab som tar beslutninger på hva som skal foretas. Dette går videre over i en etterforskning hvor politiets rolle da er å bedrive informasjonsinnsamling, herunder sikre spor og bevis.

Politiet har i dag svært begrenset operativ kapasitet som raskt kan rykke ut til virksomheter som er rammet av alvorlige digitale angrep eller på annen måte delta med politifaglig kompetanse under håndteringen. Det er et meget begrenset fagmiljø på Kripos, samt enkeltpersoner i noen få politidistrikter som i dag kan fylle en slik rolle. Det er videre i liten eller ingen grad etablert praksis for involvering av disse, og Kripos understreker at det kan ha uheldige konsekvenser for videre arbeid dersom de kommer for sent inn i sakene. Vi mister det politifaglige aspektet i håndteringen, noe som kan forsinke videre etterforskning ved at en del arbeid som for eksempel bevisinnsamling må gjøres på nytt. Det pekes i ressursgruppen også på at bevis kan ødelegges hvis det ikke tas hensyn til en mulig politietterforskning tidlig i hendelsen. NSM NorCERT har i dag av og til den rollen som politiet som regel har i fysiske hendelser og virksomheter gjør en del selv, i en del tilfeller med bistand fra leverandører.

Oppsummering av 2.5

Gap	Tiltak
Det er uforutsigbart for virksomhetene hvorvidt de får bistand fra NSM NorCERT og i så fall med hva.	3.1.1 Ambisjonsnivå 3.1.2 En plan for håndtering av digitale angrep
Politiet har i dag svært begrenset operativ kapasitet som raskt kan rykke ut til virksomheter som er rammet av alvorlige digitale angrep eller på annen måte delta med politifaglig kompetanse under håndteringen.	3.2.3 Politiet
Norske virksomheter har i for liten grad stilt krav til sine driftsleverandører når det kommer til håndtering av digitale angrep.	3.5.9 Sertifisering av leverandører 3.5.8 Lovmessige krav til leverandører
Det er generelt for lite samarbeid mellom NSM NorCERT, de sektorvise responsmiljøene og de enkelte virksomhetenes responsmiljøer.	3.2.1 Organisering
Ikke alle virksomheter hører naturlig til i et sektorresponsmiljø, enten fordi de ikke har en sterk tilhørighet til en sektor eller at det ikke finnes et sektorresponsmiljø i den sektoren.	3.2.2 Organisering av spesialiserte responsmiljøer
NSM NorCERT har ikke myndighet til å iverksette tiltak hos virksomheter i forbindelse med håndtering av digitale angrep.	3.5.5 Myndighet til å beslutte iverksettelse av tiltak

2.6 Politietterforskning

Lav grad av anmeldelser og etterforskning

Politiet etterforsker i dag i relativt liten grad kriminalitet mot data og datasystemer[4]. Det er mangel på kompetanse og kapasitet i politiet for disse sakene. Få saker anmeldes, og forventingene om at det blir etterforsket er lav. Som beskrevet over har politiet per i dag ingen operativ enhet med fokus på digitale angrep.

Anmeldelse av digitale angrep skal gå til lokalt politidistrikt, selv om det sjelden er det lokale politiet som har kompetanse til å etterforske. Hvor saken skal videre i politiet er avhengig av hvem som er trusselaktøren og hva som er intensjonen med angrepet. Etterretningstjenesten kan støtte med vurderinger av ulike trusselaktører. Kripos (ikke-statlige aktører, regulær kriminalitet), Politiets sikkerhetstjeneste (statlige aktører og terror) og Økokrim (økonomisk kriminalitet) har hver sine

[4] (Politidirektoratet, 2012)

ansvarsområder, og det er ikke alltid enkelt å avgjøre i starten hvem som skal involveres. Særlig der ansvarlig instans for å følge opp en sak er relatert til trusselaktør kan dette ta tid, ettersom det ofte er svært vanskelig å tidlig avgjøre hvorvidt for eksempel spionasje er utført av en statlig eller ikke-statlig trusselaktør. Saker må i slike tilfeller kanskje overføres mellom ulike instanser av politiet, noe som skaper mer arbeid for virksomheten som anmeldte forholdet og selve etterforskningen i politiet sett under ett tar lenger tid. Der hvor det er uklart hvilken instans i politiet som skal etterforske, kan det i tillegg være med å påvirke en beslutning om å henlegge saken.

Det er en utfordring i forbindelse med anmeldelser at det gjerne tar lang tid før politiet tar stilling til om saken skal etterforskes eller ikke. Det betyr at virksomheter potensielt må innhente og ta vare på mye informasjon til ingen nytte dersom saken henlegges. De virksomhetene som har valgt å anmelde og følge saker relatert til digitale angrep gjennom rettssystemet, opplever det som svært tidkrevende.

Ressursgruppa har diskutert hvorvidt det er et problem at ikke flere saker anmeldes. Det er i og for seg enighet om at flere saker burde kommet inn, men hensikten med anmeldelsen bør vurderes. Det stilles for eksempel spørsmål ved om en anmeldelse som ikke kan føre til en straffeprosess (for eksempel der trusselaktøren er en statlig aktør) er hensiktsmessig. Fordelen med at slike saker også blir anmeldt, er at de gir nyttig informasjon til trusselbildevurderinger. For å heve politiets fokus, kompetanse og ressurstilgang for å etterforske digitale angrep, er det også en oppfatning om at det er viktig at saker anmeldes. Flere straffesaker vil gi en større del av elektroniske bevis hvor det blir større krav til og behov for digital kompetanse i politiet.

De organisasjonene som har anmeldt digitale angrep tidligere, har gjerne etablert en relasjon og interne prosedyrer som gjør det enklere å anmelde neste gang. Usikkerhet om hvorvidt en sak vil bli etterforsket eller ikke, og hvor lang tid det vil ta, kan redusere effektiviteten på håndteringen i virksomheten som er rammet. Dersom en sak skal etterforskes av politiet, krever det gjerne andre aktiviteter enn om saken ikke politietterforskes (for eksempel kan det være situasjoner hvor mer data må sikres og lagres over lengre tid).

Internasjonale problemstillinger

Trusselaktører innenfor digitale angrep lar seg ikke begrense av nasjonale grenser. Selv om det er utstrakt samarbeid mellom både private aktører, offentlige virksomheter og politiet med internasjonale partnere, begrenses effektiviteten av at internasjonalt regelverk i liten grad er tilpasset denne typen situasjoner. Det norske politiet samarbeider med ulike internasjonale organisasjoner, for eksempel Interpol og Europol, og har eksempler på at samarbeid med disse innenfor etterforskning av trusselaktører som har gjennomført digitale angrep har vært vellykket. Effektiviteten vil imidlertid avhenge av hvilke land som er involvert. Dette er en generell utfordring innen all etterforskning, og er således ikke begrenset til digitale angrep.

Politiet er også en sterkt regulert virksomhet, som kan føre til forsinkelser i håndtering av saker. Ressursgruppa peker på det som en utfordring, men mener samtidig at det i prinsippet er riktig at politiet er sterkt regulert.

Oppsummering av 2.6

Gap	Tiltak
Få digitale angrep anmeldes til politiet.	3.2.3 Politiet 3.5.1 Enklere anmeldelser
Anmeldelser av digitale angrep henlegges i stor grad. Det kan væreuklart hvilke instans av politiet som skal etterforske en spesifikk sak.	3.2.3 Politiet
Internasjonal regelverk er i liten grad tilpasset situasjoner hvor trusselaktøren har gjennomført (forsøk på) digitale angrep i andre land.	3.5.10 Internasjonalt regelverk

2.7 Analysekapabilitet

Under analysekapabilitet forstår vi områder som undersøkelser av skadelig kode (reverse engineering), (mistenkte) infiserte maskiner (digital forensics) og logganalyse for avdekking og etterforsking.

Kapasitet

Resultatene av slike analyser kan være svært viktige for effektiviteten av håndtering av et digitalt angrep. Analysekapabiliteten i Norge er delt mellom offentlige enheter (særlig NSM NorCERT, Etterretningstjenesten og politiet) og det private (enkelte virksomheter, driftsleverandører og kommersielle sikkerhetsleverandører). Kapasiteten til Etterretningstjenesten og Politiets sikkerhetstjeneste er av sikkerhetsmessige årsaker ikke kjent, så det er vanskelig å gjøre en konkret vurdering av hvor stor kapasiteten faktisk er, men i større og/eller flere parallelle digitale angrep opplever de operative miljøene i virksomhetene som er representert i ressursgruppa at analysekapasiteten er begrenset. Manglende og forsinkede analyser kan føre til at håndteringen av en sak blir forsinket. I tillegg fører det gjerne til at beslutninger må tas på mangelfullt eller feil grunnlag, noe som igjen kan føre til økte konsekvenser av hendelsen.

Leverandørers rolle innenfor analyse

Aktører involvert i analyse i dag er som beskrevet over delt mellom det offentlige, ulike virksomheter og leverandører. Enkelte driftsleverandører leverer tjenester innenfor analyse som del av sitt tjenestetilbud, i hovedsak logganalyse. Oppfatningen i ressursgruppa er at norske virksomheter i liten grad stiller krav om denne typen tjenester til sine driftsleverandører. Hovedvekten av analysekapasitet på leverandørsiden i Norge ligger hos mer dedikerte sikkerhetsleverandører.

Ulike systemer krever ulik kompetanse

Det er også et poeng at ulike systemer er satt opp ulikt og for å gjøre effektiv analyse er det nødvendig å kjenne til hvordan systemet normalt fungerer. Det er store forskjeller på å gjøre analyse av en Windows 7-maskin og en iPhone, men begge deler kan være nødvendig i forbindelse med håndtering

av digitale angrep. Dette påvirker tiden det tar å gjøre analysen av det enkelte systemet og i praksis hvilken kapasitet vi har for å gjøre analyse som helhet.

Verktøy

Analysekapabilitet er også avhengig av verktøy. Det er få virksomheter i Norge som selv har tilgang på effektive verktøy for å innhente informasjon for analyse og gjennomføre selve analysen. Dette påvirker kvaliteten på det som gjøres, og tiden det tar å gjøre analysen.

Oppsummering av 2.7

Gap	Tiltak
I større hendelser er de operative miljøene representert i virksomhetene i ressursgruppa av den oppfatning at analysekapasitet er en begrensende faktor når det gjelder håndtering av digitale angrep.	3.1.1 Ambisjonsnivå 3.2.1 Organisering 3.4.1 Utdanning/videreutvikling
Norske virksomheter stiller i for liten grad krav til leverandører innenfor analyse.	3.4.4 Kompetanse i virksomhetene 3.5.8 Lovmessige krav til leverandører 3.5.9 Sertifisering av leverandører
Mangel på verktøy for innhenting av informasjon og selve analysen	Ressursgruppa har ikke diskutert tiltak innenfor dette området.

2.8 Kapasitet

Nasjonal mangel på ressurser

Det er i dag knapphet på personer med kompetanse på å avdekke, håndtere og etterforske digitale angrep. Dette er et problem nasjonalt, men ifølge FFIs cybermaktstudie[5] gjelder dette også internasjonalt. Nasjonalt er det særlig tydelig for fagområder innenfor analyse. Det er områder som krever mye og bred erfaring, og større fagmiljøer for å sikre tilstrekkelig utvikling og skape interessante nok arbeidsplasser til å beholde kompetansen.

Utdanninger innenfor områdene avdekke og håndtere digitale angrep tilbys i dag av ulike høyskoler og universiteter i Norge. Ved utdanningsinstitusjonene er det viktig at vi lykkes med å balansere behovet for forskning og utvikling mot utdannelsen av fagpersoner med kompetanse og ønske om å jobbe praktisk med å avdekke, håndtere og etterforske digitale angrep. Politihøyskolen samarbeider med Høyskolen i Gjøvik om å integrere verktøy og metoder knyttet til IKT i politiutdannelse, og politifaglig kompetanse i IKT-utdanning. Videre utdanner Forsvarets ingeniørhøyskole personer med kompetanse innenfor dette fagfeltet.

Det er et gap mellom den kompetansen nyutdannede, i hvert fall fra de sivile utdanningene har, og den jobben de skal gjøre. Flere deltakere i ressursgruppa stiller spørsmål ved innholdet i

[5] (Forsvarets forskningsinstitutt, 2014)

utdanningene, for eksempel om de inneholder tilstrekkelig generell IT-kompetanse, men også spesifikk kompetanse innenfor fagfeltet avdekke, håndtere og etterforske digitale angrep.

Det vi har beskrevet til nå i avsnittet begrenser oss til de som følger et spesifisert utdanningsløp fram til en bachelor eller mastergrad. Det er imidlertid flere eksempler i miljøene representert i ressursgruppa på personer som har tilegnet seg relevant kompetanse på andre måter enn gjennom de tradisjonelle utdanningene. Denne kommer ut av et sterkt engasjement og interesse for IT, og deltagelse i miljøer som bygger opp under denne interessen.

Videreutvikling

NSM NorCERT og kommersielle sikkerhetsleverandører benytter seg av studenter for å drive 24/7-overvåking. Dette er en viktig arena for å bygge opp praktisk kompetanse hos studentene. Det fungerer også som rekruttering til ulike virksomheter, både der studentene har jobbet og andre som jobber med disse problemstillingene.

Utenlandske aktører som SANS, ENISA, PECB og FIRST og ulike blogger, bøker og e-postlister er viktige kilder til oppdatert kunnskap. Ressursgruppen peker på at det er både nyttig og nødvendig at noe etterutdanning og kompetanseheving foregår internasjonalt, både for å knytte kontakter og for å sikre dagsfersk kompetanse. Samtidig er det knyttet store kostnader ved å sende ansatte på kurs i utlandet, og ressursgruppa etterspør også gode tekniske kurs og konferanser arrangert i Norge. Det oppleves som et problem at mange konferanser blir for overordnede.

Oppsummering av 2.8

Gap	Tiltak
Vi har i Norge i dag ikke tilstrekkelig med personer med riktig kompetanse som kan fylle oppgavene innenfor arbeidet med digitale angrep som beskrevet i denne rapporten.	3.4.1 Utdanning/videreutvikling 3.4.2 Rekruttering til faget
Det er for få arenaer hvor norske miljøer møtes operativt og teknisk for å bygge kompetanse og relasjoner.	3.4.3 Kurs og konferanser

2.9 Informasjonsinnhenting- og deling (nasjonalt og internasjonalt)

Innhenting og deling av informasjon er nødvendig for å effektivt kunne avdekke, håndtere og etterforske digitale angrep. Flere i arbeidsgruppa har poengtert at sikkerhet i utgangspunktet ikke er noe de konkurrerer om. Samarbeid og informasjonsdeling foregår både mellom virksomheter i samme bransje, på tvers av bransjer og mellom myndigheter, det private og Forsvaret.

Trusseletterretning

Effektiv beskyttelse av norsk infrastruktur og informasjon vil ikke kunne oppnås uten fokus både på det ukjente, men også god etterretning om ulike trusselaktører, også de som tidligere er uoppdaget mot norske mål eller der informasjon kun er tilgjengelig i graderte kanaler. Etterretning gjøres både hos ulike myndighetsfunksjoner (herunder særlig Etterretningstjenesten og Politiets

sikkerhetstjeneste), men også av private virksomheter i større og mindre grad, der fokuset på trusselaktører og relevant informasjon kan variere noe med type virksomhet.

Kanaler for deling av informasjon

Under innledende samtaler med ressursgruppas medlemmer pekte flere på at tillit er essensielt for at informasjonsdeling skal fungere. Sikkerhetsmiljøet i Norge er relativt lite, og mange er på fornavn med hverandre. Det er viktig å jobbe for at det ikke blir en «klubb» for de innvidde, men at vi klarer å beholde de personlige relasjonene samtidig som vi jobber for å inkludere alle relevante aktører. Selv om det foregår en del informasjonsdeling mellom organisasjoner, er mye av det personavhengig. Dette gjelder ikke der det er inngått formelle avtaler eller det er regelverk som styrer informasjonsdelingen.

Deltakerne i ressursgruppa deltar i ulike forum nasjonalt og internasjonalt, hvor informasjonsdeling inngår i intensjonen med forumet. Disse forumene kan være bransjespesifikke eller organisert på andre måter. Flere i ressursgruppa er medlemmer i FIRST[6], og har representanter på FIRSTs årlige konferanse. Myndighetsmiljøene representert i gruppa samarbeider med naturlige partnere innenfor sine ansvarsområder (for eksempel er en viktig oppgave for NSM NorCERT å utvikle og vedlikeholde samarbeid og informasjonsdeling med andre nasjonale CSIRT-miljøer), mens de private virksomhetene i ressursgruppa søker miljøer både nasjonalt og internasjonalt med sammenfallende problemstillinger.

NSM NorCERT samler operative miljøer i Norge i jevnlige møter. Sammensetningen av disse forumene er viktig for tilliten og dermed graden av deling i møtene. Det er også pekt på at det er relativt få av de inviterte miljøene som faktisk deler informasjon, noe som kan virke demotiverende på de som deler.

NSM NorCERT har en digital kanal (NSM NorCERT IRC), hvor operative ressurser kan dele informasjon. Dette er den kanalen vi kjenner til at tross alt fungerer best for deling av informasjon på et teknisk, operativt og nasjonalt nivå, men også her er det begrenset hvem som deler informasjon.

Gradering og klassifisering av informasjon

Informasjon relatert til digitale angrep kan av ulike årsaker være gradert i henhold til sikkerhetsloven, og kan ikke deles med ikke-autoriserte personer. Dette er gjerne informasjon som er relatert til trusselaktøren/angriperen. Det finnes også en protokoll for informasjonsdeling (trafikklysprotokollen) som brukes av operative responsmiljøer internasjonalt og nasjonalt for klassifisering av informasjon. Bakgrunnen for klassifisering i henhold til trafikklysprotokollen kan være både at den inneholder trusselaktørinformasjon eller også at den inneholder informasjon om organisasjoner som er rammet av det digitale angrepet. Det er informasjonseier som bestemmer gradering og klassifisering, og det pekes i ressursgruppa på et stort problem med at informasjon blir gradert/klassifisert for høyt, noe som hemmer informasjonsdeling og dermed mulighetene for å effektivt avdekke, håndtere og etterforske digitale angrep. Miljøene som i størst grad håndterer gradert informasjon i ressursgruppa påpeker at det jobbes kontinuerlig med å tilgjengeliggjøre mest mulig informasjon, men at det kan være tunge prosesser involvert for å få tillatelse til å dele. Det er også viktig å huske på at gradering, klassifisering og protokoller for deling gjør det mulig å dele det vi faktisk gjør, fordi det gir informasjonseier kontroll med delingen. EOS-tjenestene jobber med å følge

[6] http://www.first.org/

trusselaktører over tid for å lære om intensjoner, metoder og kapasitet, og sømløs og sanntids deling av relevant informasjon mellom disse er en viktig forutsetning for effektivt arbeid.

Antallet alvorlige spionasjesaker som håndteres i Norge har økt siden NSM NorCERT ble planlagt og etablert, og oppdagelse og håndtering av denne typen hendelser krever et nært samarbeid mellom de hemmelige tjenestene i Norge og tilsvarende samarbeidspartnere i utlandet. Dette medfører at mer informasjon er gradert i henhold til sikkerhetsloven, og det vanskeliggjør kommunikasjon og deling med ikke-klarerte personer og organisasjoner. Videre har det også vært en økning i andre typer hendelser som ikke i like stor grad krever statlig etterretningsinformasjon, slik som større banktrojanerkampanjer og andre aktiviteter med klare økonomiske motiver rettet mot Norge.

Flere av medlemmene i ressursgruppa beskriver en situasjon der NSM NorCERT oppfattes som mindre åpen nå enn de første årene, slik at samarbeid og informasjonsdeling blir mer utfordrende. NSM NorCERTs representant i ressursgruppa understreker at dette ikke er en bevisst eller villet strategi fra NSM NorCERTs side. Det er imidlertid en bekymring hos enkelte i ressursgruppa forøvrig at et slikt inntrykk på sikt kan svekke tilliten til NSM NorCERT som den nasjonale kapasiteten gruppa oppfatter at var den opprinnelige hensikten, og føre til at medlemmer og partnere i mindre grad oppfatter funksjonen som relevant og viktig for dem å ha et forhold til.

Personvern og sikkerhet

I forbindelse med informasjonsinnhenting- og deling kommer vi stadig opp i situasjoner hvor hensynet til personvern må balanseres mot hensynet til sikkerhet. For de private virksomhetene i ressursgruppa oppleves dette i relativt liten grad som et problem. De har i stor grad etablert rutiner og prosedyrer for å kunne gjennomføre de aktivitetene som er nødvendige i forbindelse med informasjonsinnhenting. mnemonic kjenner imidlertid til at dette kan være krevende for mindre virksomheter som ikke er like godt kjent med personvernregelverk og hva som er tillatt under hvilke forutsetninger.

I datanettverk finnes det mye personinformasjon, og det er viktig at informasjonsinnhenting som gjøres av politiet skjer i henhold til personvernlovgivningen og relevante hjemler. Der innhenting av informasjon gjøres, er hensynet til personvernet av domstolene veiet opp mot politiets behov, og det er sjelden et problem i praksis.

Et større problem enn selve innhentingen, er adgangen til å lagre informasjon. Politiet opplever i etterforskningen at det er svært begrensende at informasjon som kan knytte aktivitet på Internett til en person eller et abonnement ikke er tilgjengelig hos for eksempel Telenor på grunn av personvernlovgivningen. Muligheter for å innhente denne typen opplysninger, under strenge vilkår og domstolkontroll, er vesentlig for politiets evne til å etterforske, men på grunn av svært kort lagringstid (maksimum 21 dager) mister de en vesentlig primærkilde til informasjon.

Kompetanse

Informasjonsdeling er også avhengig av kompetanse, både hos den som skal dele og hos mottaker. Å forstå betydningen av informasjon krever at avsender har en god forståelse av situasjonen og kjenner sin mottaker relativt godt. Det er også en utfordring å lykkes med informasjonsdeling der mottaker har dårlig kompetanse på området. Dersom tilliten hos avsender til at mottaker håndterer mottatt informasjon riktig er lav, reduserer det vilje til å dele. Et annet problem for effektivitet og korrekt håndtering er dersom informasjonen deles, men mottaker ikke evner å utnytte den. Det er en

utfordring for informasjonsdeling og håndtering av hendelser at kompetansen i mange virksomheter rundt disse problemstillingene er for dårlig. Dette kan både handle om risiko- og konsekvensforståelse på ledernivå, teknisk IT-sikkerhetskompetanse hos utførende personer og kompetanse på håndtering av hendelser i ulike deler av organisasjonen. Vi har i ressursgruppa diskutert situasjoner der toppledelsen blir informert om det overordnede trusselbildet av Politiets sikkerhetstjeneste, de tekniske ressursene jobber sammen med NSM NorCERT og kjenner godt til den faktiske situasjonen, mens det i mellom sitter mellomledere som tar mange av de daglige avgjørelsene uten å ha tilstrekkelig kompetanse om det som skjer.

I virksomheter som ikke har erfaring med CSIRT-arbeid, er det mange ukjente begreper og protokoller. Manglende kjennskap til disse gjør det vanskelig å reagere på hensiktsmessig måte.

Det er også viktig å poengtere at ressursgruppa består av representanter fra store organisasjoner med relativt store og modne interne miljøer involvert i problematikk rundt digitale angrep. Mindre organisasjoner vil i enda større grad påvirkes av personavhengighet og mangel på kompetanse til å håndtere den informasjonen de har tilgjengelig. Dette er en utfordring, for disse er en viktig del av den helhetlige sikkerheten i Norge. De kan for eksempel utnyttes av trusselaktører i angrep mot større virksomheter, noe vi har sett flere eksempler på det siste året. I tillegg er det flere mindre virksomheter i Norge som forvalter samfunnsviktig infrastruktur og informasjon.

Oppsummering av 2.9

Gap	Tiltak
Informasjonsdeling er i Norge i dag i stor grad personavhengig. Dette er en styrke på enkelte områder, men det er behov for noe mer struktur for å sikre at alle relevante miljøer tar del i informasjonsdelingen.	3.4.4 Kompetanse i virksomhetene 3.4.3 Kurs og konferanser
Innenfor arbeid med alvorlige digitale angrep og særlig statlige trusselaktører er det mye gradert informasjon. Måten vi organiserer håndteringen av hendelser på i dag, gjør at de som håndterer hendelsen i mindre grad har tilgang på denne informasjonen, noe som reduserer effektiviteten av håndteringen.	3.1.1 Ambisjonsnivå 3.1.2 En plan for håndtering av digitale angrep 3.2.1 Organisering
Forståelse hos beslutningstakere på ulike nivåer i norske virksomheter er ikke tilstrekkelig.	3.4.4 Kompetanse i virksomhetene 3.4.3 Kurs og konferanser
Det er begrensninger i hva som tillates lagret og hvor lenge begrunnet i personvern. Dette påvirker politiets (og virksomhetenes) evne til å etterforske digitale angrep.	3.5.6 Sikkerhet og personvern

3 Tiltak

3.1 Strukturelle

Innenfor området strukturelle tiltak har vi plassert tiltak som går på overordnede forhold med betydning for måten vi organiserer og arbeider med digitale angrep.

3.1.1 Ambisjonsnivå

Innenfor området avdekke, håndtere og etterforske digitale angrep har ressursgruppa som beskrevet i vanskelig for å se tydelige ambisjoner og forventninger fra øverste myndigheter.

Ressursgruppa mener med bakgrunn i dette at det må gjøres gjennom en grundig kartlegging av de verdiene Norge ser på som viktige. Kartleggingen og definisjonen av samfunnskritiske funksjoner kan etter gruppas mening i denne sammenhengen ikke knyttes til begrepene i Forskrift om objektsikkerhet, og må gjøres uavhengig og tverrsektorielt. Det ble i gruppa diskutert ulike konsekvenskriterier for å vurdere hva som er samfunnskritisk. Det ble for eksempel pekt på eksempler i land hvor en hendelse kategoriseres som alvorlig dersom den rammer en viss prosentandel av befolkningen. Dette blir ikke ansett som en hensiktsmessig måte å definere det på, for eksempel fordi det kan være funksjoner som ikke er kritiske for samfunnets funksjon, men som allikevel kan ha stor symbolverdi. Videre diskuterte ressursgruppa at det ikke er innenfor vår oppgave å bestemme kriterier eller gjøre en slik kartlegging.

Basert på verdivurderingen må myndighetene være tydelige på hvilke ambisjoner de har for nasjonal håndtering av ulike typer situasjoner og digitale angrep. Det må tydelig beskrives hvilke oppgaver som ligger til ulike myndighetsfunksjoner, slik at virksomhetene vet hva de kan forvente at håndteres nasjonalt, og hvor det er behov for egne aktiviteter.

En slik aktivitet må gjøres av en instans eller et organ som evner å se hensyn på tvers av sektorer og har tilstrekkelig myndighet til å si noe om hva som er kritisk for Norge.

3.1.2 En plan for håndtering av digitale angrep

Etter at ambisjonsnivået for myndighetenes involvering i ulike former for digitale angrep er klar, må det lages planer for å håndtere de ulike situasjonene. God praksis[7] tilsier at en slik plan blant annet må inneholde:

- Strategier og målsetninger
- Godkjennelse av øverste ledelse
- Organisatorisk tilnærming – videre beskrevet i 3.2.1 Organisering
- Kommunikasjonsplan for interessenter internt og eksternt
- Parameter for måling av kapabilitet og effektivitet
- Sammenhengen med andre prosesser og rammeverk – for eksempel generelle beredskapsplaner

[7] (NIST - National Institute of Standards and Technology)

Selv om dokumentet fra NIST er laget for organisasjoner og virksomheter, er dette nyttige temaer å ha med seg også for nasjonal kapasitet.

3.1.3 Prinsipielt skille på tilsyn og operative enheter

Dersom tilsyn og operative enheter skal fungere i samme organisasjon, stiller det krav til at myndighetsfunksjonen er svært god på å skille de to områdene fra hverandre. Dersom en ikke lykkes med det, vil det innvirke på tilliten virksomheten underlagt tilsynsmyndigheten har til den operative enheten.

I Norge er det foreløpig ett eksempel hvor det operative responsmiljøet er organisatorisk plassert sammen med en tilsynsmyndighet, nemlig NSM NorCERT som en funksjon i NSM. Ressursgruppa har ikke gått i detalj inn i å undersøke hva dette har for eksempel for rapportering av hendelser til NSM NorCERT fra selskaper underlagt sikkerhetsloven.

Prinsipielt mener ressursgruppa allikevel at tilsyn og operative enheter ikke bør være plassert i samme myndighetsfunksjon.

Enkelte av gruppas medlemmer uttalte seg ikke om dette spørsmålet.

3.2 Organisatoriske

Ressursgruppa mener det er nødvendig å se på hvordan vi organiserer kapasiteter som i dag er involvert i å avdekke, håndtere og etterforske digitale angrep for å bruke de ressursene vi har tilgjengelig mer effektivt. Hvordan det er hensiktsmessig å organisere den nasjonale kapasiteten vil imidlertid avhenge av myndighetenes ambisjonsnivå, se foregående avsnitt.

3.2.1 Organisering

Ressursgruppa er noe uenige i hvor mye kapasitet staten skal bygge opp. Deler av gruppa mener at staten i større grad må være involvert i håndtering, ettersom en del tekniske indikatorer må ses både i sammenheng med andre pågående kampanjer og kjente trusselaktører som EOS-tjenestene i hovedsak vil ha kjennskap til. Andre deler av gruppa mener dette kan løses gjennom bedre informasjonsdeling til virksomheter og drift- og sikkerhetsleverandører, ikke minst fordi en slik løsning sannsynligvis vil skalere bedre enn at staten skal bygge opp kapasitet til å håndtere alt. Etterretningstjenesten mener det er lite realistisk å anta at høygradert etterretningsinformasjon skal deles utenfor etablerte kanaler og bruksbegrensninger.

Det er i denne sammenhengen også viktig å se på politiets rolle i forbindelse med arbeid med digitale angrep i Norge. Som beskrevet i 2.5, er ikke politiets nødvendigvis tilstede i håndteringen av et digitalt angrep, og i hvert fall ikke i en tidlig fase. Representanter i ressursgruppa ønsker seg et politi som i større grad kan ta samme rolle i forbindelse med digitale angrep som de har i fysiske hendelser.

Det er derfor vanskelig å gi en entydig anbefaling når det gjelder hvordan den nasjonale kapasiteten for «håndtering av alvorlige dataangrep» skal organiseres. Vi har i ressursgruppa diskutert ulike hensyn som må balanseres i måten vi organiserer den nasjonale kapasiteten for å avdekke, håndtere og etterforske digitale angrep:

- Det må være klart hvilke type situasjoner ulike funksjoner skal være involvert i
- Myndighetenes bidrag og ambisjoner må være tydelig avklart

- Roller og ansvar mellom ulike funksjoner må være klart definert
- Samarbeid mellom ulike virksomheter, sektorvise responsmiljøer og andre aktører
- Vi må jobbe for å kunne håndtere både gradert og ikke-gradert informasjon effektivt
- Vi trenger å bygge opp tilstrekkelig sterke fagmiljøer

Ressursgruppa mener videre at tilstrekkelig analysekapabilitet krever at vi samler ressursene i gode og store miljøer, slik at personene gis tilstrekkelig med arbeid slik at kompetansen kan vedlikeholdes. Større miljøer kan også prioritere å bygge opp kompetanse på smalere områder (for eksempel mindre utbredte systemer), fordi de tross alt oftere vil treffe på behov for analyse innenfor disse områdene.

Et forslag ressursgruppa har diskutert er opprettelsen av ett senter som skal avdekke, håndtere og etterforske ulike former for digitale angrep, der en del av senteret har et særskilt ansvar for å koordinere mot de hemmelige tjenestene, mens resten av senteret jobber med andre typer saker.

Hvis et slikt senter skal fungere, må det ha et tydelig definert oppdrag og mandat, og rapportere på oppnåelse av helt spesifikke kriterier. Dette må igjen henge sammen med myndighetenes ambisjonsnivå som beskrevet over. Viktige momenter å beslutte i forbindelse med opprettelse av et slikt senter er:

- Hvem skal bemanne det?
- Hvilken beslutningsmyndighet har senteret?
- Hvordan håndteres gradert informasjon internt i senteret?
- Hvor får senteret informasjon fra?
- Hvordan kan det legges til rette for effektiv informasjonsdeling internt i senteret og til relevante aktører?
- Hvilken kapasitet skal senteret ha?

Dette senteret bør har ett kontaktpunkt, med effektive funksjoner og prosesser for fordeling av saker og tilbakemeldinger til de som melder inn saker.

Et slik senter kan for eksempel etableres som en statlig finansiert ikke-kommersiell stiftelse. Den kan for eksempel drives at et styre bredt sammensatt av interessenter med kompetanse innenfor stiftelsens ansvarsområde. Styrets viktigste oppgave må være å skape en fleksibel organisasjon som kan reagere raskere på endringer i trusselbilde enn statlige funksjoner kan gjøre i dag, samtidig som den må holde seg innenfor de rammene som er satt av myndighetene.

Et alternativ til et slikt senter er at organiseringen i stor grad beholdes som den er i dag. Det krever at NSM NorCERTs rolle beskrives tydeligere og at det i større grad kommuniseres hva andre aktører kan forvente av funksjonen. De sektorvise responsmiljøene blir i en slik organisering viktige, og det må gjøres grep for å inkludere flere virksomheter i slike miljøer, for at informasjonsdeling kan gjøres på en mer effektiv måte i virksomheter som står overfor sammenfallende problemstillinger uavhengig av sektortilhørighet. Det må også opprettes sterkere koblinger mellom de ulike sektorvise responsmiljøene enn det som finnes i dag. Der det er mulig, bør de fysisk samlokaliseres med NSM NorCERT. Der det ikke er mulig eller ønskelig, bør det legges til rette for sterkt samarbeid gjennom digitale samhandlingsløsninger. Å fortsette med samme organisering som i dag fritar ikke

myndighetene fra å gjøre avklaringer rundt roller og ansvar i forbindelse med digitale angrep. En viktig del av dette er myndighetenes ambisjoner rundt politiets rolle.

Uavhengig av hvilke organisasjonsform som velges, bør det legges opp til at de statlige funksjonene rapporterer på kritiske parameter for å verifisere at funksjonen gjennomfører de oppgaver den er tildelt. Dette må være målrettet og enkelt, slik at funksjonen ikke bruker uforholdsmessig tid på å rapportere, og oppfølgingen av rapporteringen må ha som hensikt å forbedre funksjonen. Hvilke parameter det rapporteres på må komme som en følge av ambisjoner og modenhet, men mulige parameter inkluderer[8]:

- Antall hendelser håndtert (krever kategorisering av hendelser og tydelig beskrivelse av hva som menes med håndtert)
- Tid brukt per hendelse (total arbeidstid, tid som har gått fra sak ble opprettet til den ble avsluttet, initiell responstid)
- Evaluering av spesifikke hendelser (objektiv og subjektiv evaluering)

Som for all annen type måling og rapportering, må kriteriene vurderes opp mot hva man faktisk ønsker å oppnå, og når kriteriene settes må det være høy bevissthet rundt hvordan det vil påvirke funksjonens virke. Dersom funksjonen måles på hvor lang tid den bruker fra en sak er opprettet til den er avsluttet, må kriteriene for når en sak kan avsluttes være helt klare.

3.2.2 Organisering av spesialiserte responsmiljøer

I dag er det i Norge som vi har beskrevet et fokus på å etablere sektorvise responsmiljøer. I ressursgruppa har vi diskutert om det er andre kriterier for tilhørighet i en spesifikk sektor som bør ligge til grunn for et samarbeid gjennom et spesialisert responsmiljø. For eksempel vil kraftselskapene som nå etablerer KraftCERT ha mange sammenfallende tekniske utfordringer som selskaper i olje- og gassektoren. Videre vil virksomheter innenfor ulike sektorer kunne stå overfor et likere trusselbilde enn virksomheter innenfor samme sektor.

Kriterier for organisering av slike spesialiserte responsmiljøer kan være for eksempel:

- Trusselbildet
- Angrepsvektorer
- Aktører

Her mener vi at de ulike sektormyndighetene, inkludert tilsynsmyndigheter, spiller en viktig rolle i å oppfordre til samarbeid på tvers av sektorer, ikke minst gjennom selv å samarbeide innenfor disse temaene.

3.2.3 Politiet

For politiet er det for å være bedre rustet innenfor arbeidet med digitale angrep nødvendig å bygge en sentralisert ressurs med mer kapasitet og kompetanse enn hva som er tilfellet i dag, men det er også behov for økt kapasitet og kompetanse i distriktene. I dag er det en stor mangel at politiet i liten grad har operative ressurser som kan bidra med politifaglig kompetanse i disse sakene mens de foregår og dersom det opprettes ett senter for å arbeide med digitale angrep som beskrevet i avsnittet over, bør

[8] (NIST - National Institute of Standards and Technology)

politiressurser inngå i dette senteret. Et digitalt angrep vil kunne være avsluttet i løpet av minutter eller timer, med mindre ett av målene er persistent tilstedeværelse. Det betyr at en politifunksjon må for alle praktiske formål være operativ 24/7 og i stand til å støtte umiddelbart, dersom ikke et slikt ansvar skal tildeles et nasjonalt senter. En av ressursgruppens medlemmer mente det var på tide å etablere et særorgan i politiet innenfor digitale angrep, slik ØKOKRIM i sin tid ble opprettet for å løfte arbeid mot miljø- og økonomisk kriminalitet.

Et tettere samarbeid mellom ulike politimyndigheter kan gjøre det enklere for de lokale politidistriktene å rute anmeldelser videre, ettersom de da ikke trenger samme kompetanse på å vurdere hva som er riktig instans før de videreformidler saken.

For videre vurderinger og refleksjoner rundt dette tiltaket, henviser vi til rapporten Politiet i det digitale samfunnet[9], samt videre utredninger som gjøres i Politidirektoratet parallelt med arbeidet med denne rapporten.

3.3 Teknologiske

3.3.1 Deteksjonsmekanismer

Som beskrevet over er det ingen krav til noen virksomheter om å delta i VDI-sensornettverket. Det er også viktig å være klar over at full VDI-dekning selv i enkelte virksomheter er urealistisk. Et eksempel på utfordringene rundt dette er at mange store norske selskaper har utstrakt virksomhet både i Norge og utlandet, og nettverkene kan være bygd på en slik måte at det er svært mange internett-linker. Effekten ved å plassere en sensor per tilkoblingspunkt vil da neppe forsvare kostnaden. I tillegg vil det være en begrensning på hvilken kryptert trafikk VDI-sensorene vil kunne se. Flere av representantene i ressursgruppa er opptatt av at virksomheter ikke skal få inntrykk av at med VDI-sensor og andre tjenester fra NSM NorCERT trenger de ikke å ha et forhold til egen sikkerhet.

Det kan vurderes om enkelte virksomheter skal pålegges deltakelse i VDI-sensornettverket, og i så fall om finansieringsmodellen må endres. Etterretningstjenesten mener også at det må vurderes om samarbeidet mellom EOS-tjenestene kan styrkes ytterligere, herunder styrket informasjonsdeling og sensorsamarbeid. Det er også viktig å vurdere utbredelsen av graderte sensorer, som kan utnytte gradert etterretningsinformasjon om trusselaktører.

For å effektivisere antall sensorer og mengden trafikk de ser, kan et alternativ være å plassere sensorer i knutepunkter for internettkommunikasjon i Norge. Deteksjonsmekanismene må tilpasses ambisjonsnivået som beskrevet over.

Etterretningstjenesten mener at for å avdekke og bidra til håndteringen av de mest alvorlige trusler i det digitale rom, andre staters spionasjevirksomhet og eventuelle forberedende sabotasjetiltak, er det det nødvendig å etablere en statlig etterretningsfokusert kapasitet for deteksjon, attribusjon og bistand til defensiv hendelseshåndtering knyttet til elektronisk kommunikasjon som går inn og ut av Norge. En slik form for digital grensekontroll krever ny lovgivning, som også ivaretar personvern og andre grunnleggende menneskerettigheter.

[9] (Politidirektoratet, 2012)

3.3.2 Automatisert deling av indikatorer

Effektiv deling av tekniske hendelsesdata mellom ulike organisasjoner, kan redusere den totale konsekvensen av et digitalt angrep betydelig, både ved at de kan brukes til avdekking på et tidlig stadium, men også fordi de kan brukes for analyse i en hendelse.

Deling av indikatorinformasjon er tidkrevende å gjennomføre manuelt og det bør derfor være et mål å gjøre mer automatisert deling av indikatorer. Dette er et område det jobbes mye med internasjonalt, og det er utviklet ulike protokoller og verktøy for å implementere dette. For eksempel har FS-ISAC (organisasjon som jobber med informasjonsdeling innenfor finansbransjen i USA), nettopp lansert et produkt som har implementert protokollen STIX/TAXII for automatisert informasjonsdeling[10]. Også ulike miljøer i Norge jobber med prosjekter for automatisert deling av indikatorer. I den forbindelse er det viktig at miljøene snakker sammen, slik at det ikke tas valg i en tidlig fase som reduserer mulighetene og effektiviteten i forbindelse med automatisert deling av indikatorer.

Per i dag kan de færreste organisasjoner ta imot automatisert deling av indikatorer. For eksempel KraftCERT ser imidlertid på det som en viktig oppgave å kunne ta imot strømmer av indikatorer og omsette dem til signaturer på vegne av sine medlemmer. Leverandører av sikkerhetsmonitoreringstjenester kan være viktig for implementering og utbredelse av automatisert deling av indikatorer.

Det bør vurderes om NSM NorCERT eller andre offentlige funksjoner kan tilby infrastruktur for å bedre automatisert informasjonsdeling.

3.4 Kompetansemessig

3.4.1 Utdanning/videreutvikling

Det er viktig at vi lykkes med å rekruttere de riktige ressursene, og gir dem den kompetansen de har behov for. Sammenslåingen av NTNU og HiG kan gi gode resultater, gitt at den medfører mer samarbeid og utvikling av sterke bachelor- og masterprogrammer innenfor fagfeltet. I tillegg bør utdanningsinstitusjonene i størst mulig grad søke samarbeid med arbeidslivet. Utviklingen innenfor IT-sikkerhet og digitale angrep går raskt, og akademia må bestrebe seg på å tilby mest mulig oppdatert kunnskap.

Samarbeid mellom arbeidsliv og utdanningsinstitusjonene er også svært viktig. Både NSM NorCERT og private virksomheter benytter seg av studenter i forbindelse med sine overvåkingstjenester. Dette gir praktisk kompetanse til studentene, og kan være et viktig steg for å forberede dem til arbeidslivet senere.

Ressursgruppa foreslår å vurdere om det kan utarbeides formelle programmer for videreutvikling av de som utdannes innenfor informasjonssikkerhet som en slags praksis/trainee-ordning.

3.4.2 Rekruttering til faget

Rekruttering og interesse må starte tidlig, og det kan være interessant å se mot for eksempel Storbritannia, hvor et ikke-kommersielt selskap kalt Cyber Challenge UK (http://cybersecuritychallenge.org.uk/) jobber med skolebarn for å vekke og øke interessen for fremtidige karrierer innenfor IT-sikkerhet.

[10] http://www.soltra.com/

Også det norske initiativet «Lær kidsa koding» kan være interessant å se nærmere på og gi støtte fra både myndigheter og andre miljøer.

3.4.3 Kurs og konferanser

Ressursgruppa ønsker seg flere målrettede og teknisk gode kurs og konferanser i Norge, både for å slippe reisekostnader, men også for å i større grad kunne samle sikkerhetsmiljøet er Norge. Disse bør ha som formål å øke kompetansen til menneskene som jobber innenfor dette fagfeltet, mer enn at det får et kommersielt fokus.

3.4.4 Kompetanse i virksomhetene

UNINETT CERT gjør opplæring av sine medlemmer i grunnleggende CSIRT-kompetanse. Dette bør også gjøres for andre sektorer og virksomheter, gjerne som en del av medlemsprosessen. Det bør defineres et minimum som alle skal kjenne til, for eksempel trafikklysprotokollen og viktige aktører innenfor fagområdet i Norge. Utarbeidelse og oppdatering av kursmateriale kan gjerne ligge hos NSM NorCERT, men det å holde kurset kan gjerne distribueres for eksempel til de ulike sektor-CSIRTene i forbindelse med medlemsmøter eller lignende.

Kurset bør gjennomføres med personlig oppmøte, men kan også med fordel gjøres tilgjengelig som e-læring for de som har deltatt. Det bør også gjøres tilgjengelig for virksomheter og funksjoner som ikke har tilhørighet i en sektor-CSIRT.

3.4.5 Gjennomføring av øvelser

Prosesser og prosedyrer må etableres, forankres og implementeres i forkant av øvelsene. I tillegg til store øvelser med mange involverte, bør det gjennomføres flere og mindre øvelser. Dette kan også i større grad gjenbrukes i mindre virksomheter som sjelden inviteres inn i de store koordineringsøvelsene fra myndighetene.

Dette kan være en viktig oppgave for de sektorvise responsmiljøene, men må i utgangspunktet favne bredere enn de som har en tydelig sektortilhørighet.

3.4.6 Læring etter hendelser

Det er viktig at læring etter hendelser gjennomføres med alle involverte parter. Der NSM NorCERT er involvert i håndtering av hendelser, foreslår ressursgruppa at NSM NorCERT eller tilsvarende funksjon får et særskilt ansvar for å sørge for at evaluering og læring gjennomføres i etterkant med alle involverte parter. For å sikre at det prioriteres og at det er tilstrekkelige ressurser tilgjengelig i NSM NorCERT for å gjøre det, kan det inngå som del av evalueringskriterier de må rapportere på.

3.5 Regulatoriske

3.5.1 Enklere anmeldelser

Ressursgruppa foreslår å se på muligheten for å lage et system for enklere anmeldelser med en garantert frist for tilbakemeldinger innen få dager på hvorvidt politiet henlegger eller ønsker å gjøre etterforskning. Med bakgrunn i tilbakemeldingen kan bedriften gjøre nødvendig innhenting av informasjon der det er nødvendig og ikke i alle tilfeller. Kripos sin representant i ressursgruppa er usikker på hvordan dette vil fungere i praksis.

3.5.2 Rapportering av hendelser

Det bør vurderes om norske virksomheter skal pålegges rapporteringsplikt for informasjonssikkerhet og hendelser på lik linje med finans og HMS. Det må i så fall lages gode retningslinjer for hva som skal rapporteres og det må være tydelig hva rapporteringen skal brukes til. Hensikten med et slikt tiltak vil være å øke ledelsens oppmerksomhet på problemstillingene, og forhåpentligvis løfte nivået på sikkerheten.

3.5.3 Oppdatering av lover og regler

Det bør gjøres en gjennomgang av relevante lover og regler for å sikre at de er oppdatert med tanke på endringer i risikobildet knyttet til digitale angrep. I en slik prosess bør det også fokuseres på at lovverket må støtte opp under arbeid med digitale angrep, og ikke pålegge virksomhetene aktiviteter og tiltak som ikke øker sikkerheten.

En slik gjennomgang bør gjøres av ressurser med både juridisk bakgrunn og deltagere fra operative miljøer for å avdekke, håndtere og etterforske digitale angrep. Ressursgruppa har ikke hatt tid til å gå i detaljer på dette området.

3.5.4 Felles basis for regelverk på tvers av bransjer

Regelverk relatert til for eksempel logging i dag har ikke en felles basis. Det bør vurderes om det er behov for en samkjøring av regelverk, og at det stilles noen minimumskrav på tvers av sektorer. Ressursgruppa har ikke hatt tid til å gå inn i detaljer på dette området.

3.5.5 Myndighet til å beslutte iverksettelse av tiltak

NSM NorCERT mener at en nasjonal funksjon trenger mekanismer for å pålegge virksomheter iverksettelse av enkelte tiltak for å kunne håndtere hendelser effektivt. Politiet har dette per i dag i noen grad gjennom politilovens hjemler, men det kan være behov for en slik myndighet også i kartleggingsarbeid og før det foreligger anmeldelser.

Dette er det ikke enighet om i gruppa. Flere stiller spørsmål ved at staten skal ha myndighet til å iverksette tiltak hos den enkelte virksomhet. En slik beslutningsmyndighet krever uansett veldig klare retningslinjer for når den utløses, samt svært god kompetanse både på konsekvenser hos den enkelte virksomhet og for samfunnet hos de som settes til å forvalte en slik myndighet.

3.5.6 Sikkerhet og personvern

Sikkerhet må balanseres mot personvern. I en del situasjoner opplever ressursgruppa at hensynet til personvern veier tyngre enn hensynet til sikkerhet. Vi mener derfor det er behov for å gjøre en prinsipiell vurdering av hvordan disse skal håndteres mot hverandre i forbindelse med å avdekke, håndtere og etterforske digitale angrep.

Mange demokratiske land søker også etter egnede mekanismer for å ivareta balansen mellom nasjonal beskyttelsesevne og personvern. En mulighet er at man har høyere grad av beskyttelse på visse typer kritiske systemer, arbeidsplasser og nett, hvor brukere gir informert samtykke. Et eksempel på systemer som allerede har det i dag er Forsvarets graderte nett.

En av gruppas medlemmer spør om avdekking og håndtering av digitale angrep skal unntas fra personvernlovgivning og heller reguleres i eget lovverk. Dette er ikke diskutert i ressursgruppa, men vi oppfordrer juridiske eksperter på personvernlovgivning til å se videre på denne problemstillingen.

3.5.7 Enklere bistandsanmodninger?

I dag er veien til bistand fra Forsvaret i en hendelse i sivil sektor relativt lang, ettersom det krever en bistandsanmodning. Dersom det er et mål at sivil sektor i større grad skal benytte Forsvarets apparat, må prosessen og tidsbruken rundt bistandsanmodninger forenkles.

3.5.8 Lovmessige krav til leverandører

Det er i dag et lite utvalg leverandører som utgjør infrastrukturen til mange samfunnsviktige funksjoner i Norge. Det er kundens ansvar å stille riktig krav til sine leverandører, og det er kundens ansvar å være i henhold til gjeldende lovverk i sin sektor. Dog er det ressursgruppen bekjent ikke noen som vurderer driftsleverandørenes totale sum av kunder og konsekvenser ved digitale angrep.

Vi foreslår å vurdere om driftsleverandørene bør underlegges egne lovmessige krav for å sikre at de løser sine oppgaver på best mulig måte for Norge.

3.5.9 Sertifisering av leverandører

Det bør vurderes om det skal gjøres sertifisering av leverandører, både de som leverer driftstjenester og mer rene sikkerhetsleverandører. For at denne typen sertifisering skal gi mening, må det ligge klare kriterier til grunn. Den må være målrettet nok og fokusere på de områdene som oppfattes som viktige. En mulighet er å basere seg på allerede eksisterende sertifiseringsordninger, slik som ISO/IEC 27001. Ved bruk av ISO/IEC 27001 må det verifiseres at hele den delen av virksomheten som er relevant for tjenestene som skal leveres, inngår i omfanget av sertifiseringen.

Sertifiserte leverandører kan enten være et tilbud til de virksomhetene som ønsker det, eller det kan være et krav til enkelte virksomheter å benytte sertifiserte leverandører.

3.5.10 Internasjonalt regelverk

Innenfor dette området er det svært krevende å skissere tiltak som gir effekt, ettersom dette avhenger av en rekke faktorer norske myndigheter ikke selv har kontroll med. Vi er avhengige av konsensus og at noen til en viss grad gir slipp på suverenitet og jurisdiksjon. Ressursgruppa begrenser seg derfor til å fremheve betydningen av å ta en aktiv rolle i arbeidet med å forenkle og fornye de konvensjonene som regulerer internasjonalt samarbeid ved etterforskning.

4 Metode

4.1 Deltakere

Organisasjon	Kontaktperson	Rolle
DNB	Anders Hardangen	Ressursgruppemedlem
Statoil	Karl Martin Sola	Ressursgruppemedlem
Kongsberggruppen	Terje Vernholt/Johnny Løcka	Ressursgruppemedlem
PST	Lars Olav Hirth Sausjord	Ressursgruppemedlem
Kripos	Thomas Stærk	Ressursgruppemedlem
Statnett	Margrete Raaum	Ressursgruppemedlem
Etterretningstjenesten	Marianne Aas	Ressursgruppemedlem
Telenor	Rune Dyrlie	Ressursgruppemedlem
NSM NorCERT	Tor Saltveit/Pål Arne Hoff	Ressursgruppemedlem
Watchcom	Roar Sundseth	Fasilitator
mnemonic	Mona Elisabeth Østvang	Fasilitator
mnemonic	Siri Bromander	Fasilitator

4.2 Aktiviteter

Informasjon til rapporten er innhentet gjennom ulike aktiviteter. Det ble først gjennomført samtaler med de enkelte ressursgruppemedlemmene. Deretter ble alle samlet til 3 arbeidsmøter, hvor nå-situasjon, gap og tiltak ble diskutert. Grunnlaget for samtalene og arbeidsmøtene med utgangspunkt i dokumentene listet i referanselista i kapittel 5 i denne rapporten.

Det ble så utarbeidet en rapport som har vært på to tilbakemeldingsrunder i ressursgruppa og til kontaktpersoner i Lysneutvalget.

4.3 Versjonskontroll

Dato	Versjon	Endring utført av	Årsak til endring
06.01.15	0.1	Mona Elisabeth Østvang	Dokument opprettet
28.01.15	0.2	Mona Elisabeth Østvang	Dokument oppdatert etter første arbeidsmøte
04.02.15	0.3	Mona Elisabeth Østvang Siri Bromander	Dokument oppdatert etter andre arbeidsmøte
05.02.15	0.5	Mona Elisabeth Østvang Siri Bromander	Dokument oppdatert etter tredje arbeidsmøte
20.02.15	0.6	Mona Elisabeth Østvang Siri Bromander	Dokument oppdatert etter første tilbakemeldingsrunde fra ressursgruppa
27.02.15	0.9	Mona Elisabeth Østvang Siri Bromander Kvalitetssikring mnemonic: Gjermund Vidhammer	Dokument oppdatert etter andre tilbakemeldingsrunde fra ressursgruppa og kontaktpersoner Lysneutvalget
20.03.15	1.0	Mona Elisabeth Østvang	Rapport ferdigstilt.

5 Referanser

Christopher J. Alberts, A. J. (2014, May). *An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC).* Hentet fra Software Engineering Institute, Carnegie Mellon University: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=91452

Direktoratet for sikkerhet og beredskap. (2012). *Sikkerhet i kritisk infrastruktur.* Hentet fra http://www.dsb.no/Global/Publikasjoner/2011/Rapport/KIKS.pdf

Fornyings- administrasjons- og kirkedepartementet. (2012). *Handlingsplan - nasjonal strategi for informasjonssikkerhet.* Hentet fra www.regjeringen.no: https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf

Fornyings-, administrasjons-, og kirkedepartementet. (2012, Desember). *Nasjonal strategi for informasjonssikkerhet.* Hentet fra www.regjeringen.no: https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

Forsvarets forskningsinstitutt. (2014). Hentet fra www.ffi.no: http://www.ffi.no/no/rapporter/13-02712.pdf

mnemonic AS. (2015). *Sikkerhetsåret 2015.* mnemonic AS. Hentet fra www.mnemonic.no: Ikke publisert enda

NIST - National Institute of Standards and Technology. (u.d.). *Computer Security Incident Handling Guide.* Hentet fra http://csrc.nist.gov/: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Næringslivets sikkerhetsråd. (2014). *Mørketallsundersøkelsen.* Hentet fra www.nrs-org.no: http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014.pdf

Politidirektoratet. (2012). *Politiet i det digitale samfunnet.* Hentet fra Politidirektoratet: https://www.politi.no/vedlegg/rapport/Vedlegg_1866.pdf

Traavikutvalget. (2012). *Ekstern gjennomgang av Politiets sikkerhetstjeneste.* Hentet fra www.regjeringen.no: https://www.regjeringen.no/globalassets/upload/jd/dokumenter/rapporter/2012/ekstern_gjennomgang_av_pst.pdf