FORSVARSDEPARTEMENTET

Forsvarsdepartementets strategi for informasjonssikkerhet i forsvarssektoren

«Informasjonssikkerhetsstrategi for forsvarssektoren»

Informasjonssikkerhetsstrategi for forsvarssektoren fastsettes for bruk i Forsvarsdepartmentet og underlagte etater

Oslo, 1. februar 2017

Erik Lund-Isaksen
Departementsråd
Forsvarsdepartementet

Metadata

KORTTITTEL:	Informasjonssikkerhetsstrategi for forsvarssektoren
SIKKERHETSGRADERING:	Ugradert
IKRAFTTREDELSE:	25. februar 2017
HJEMMEL:	Organisasjons- og instruksjonsmyndigheten
ANSVARLIG FAGMYNDIGHET:	Forsvarsdepartementet
GJELDER FOR:	Forsvarsdepartementet og underlagte etater
FORRIGE VERSJON:	

Innhold

1. Innledning

Hensikten med denne strategien er å styrke informasjonssikkerheten i forsvarssektoren. Strategien skal også bidra til å styrke informasjonssikkerheten hos forsvarssektorens leverandører og sentrale samarbeidspartnere gjennom tverrsektorielt samarbeid.

Informasjonssikkerhet omfatter både informasjon og informasjonssystemer, uavhengig av om informasjonen produseres og formidles i digitalt format, i fysisk format eller i form av tale, eller om informasjonen flyttes mellom ulike formater. Tap, kompromittering eller endring av informasjon kan få alvorlige konsekvenser for nasjonen, for virksomheter eller for enkeltpersoner. Informasjons-sikkerhet er derfor en grunnpilar for en forsvarlig informasjonsforvaltning.

En overordnet målsetting for arbeidet med informasjonssikkerhet i forsvarssektoren er at:

> ***God informasjonssikkerhet skal bidra til at forsvarssektoren kan løse sine oppgaver i fred, sikkerhetspolitisk krise og væpnet konflikt.***

På overordnet nivå handler informasjonssikkerhet om å sikre informasjonens:

- Konfidensialitet (hindre at uvedkommende får tilgang til informasjonen)
- Integritet (hindre at informasjonen blir endret uten tillatelse)
- Tilgjengelighet (hindre bortfall av tilgangen til informasjon)
- Sporbarhet[1] (finne ut hvem som har håndtert informasjonen og hvordan den har blitt håndtert)

Disse fire prinsippene er likestilte, og må sees i sammenheng. Mangler innenfor ett av prinsippene kan ikke nødvendigvis kompenseres ved å styrke et av de andre.

Informasjonssikkerhet er en forutsetning for sikker produksjon, lagring, tilgjengeliggjøring og forsendelse av informasjon. Beslutningstakere i forsvarssektoren er avhengige av at rettidig og pålitelig informasjon formidles til autorisert personell gjennom våpenplattformer, kommando- og kontrollsystemer og andre informasjonssystemer. Mangelfull eller feil informasjon vil redusere evnen til å fatte gode og rettidige beslutninger. En forsvarlig informasjonsforvaltning er således et viktig premiss for Forsvarets operative evne og for virksomhetenes evne til å løse sitt samfunnsoppdrag. Forståelsen for viktigheten av informasjonssikkerhet må ligge i virksomhetskulturen. Det må iverksettes hensiktsmessige og kostnadseffektive sikkerhetstiltak for å beskytte forsvarssektorens informasjon og informasjonssystemer.

[1] Informasjonssikkerhet deles tradisjonelt inn i konfidensialitet, integritet og tilgjengelighet. Det digitale sårbarhetsutvalget (Norges offentlige utredninger 2015:13 Digital sårbarhet – sikkert samfunn. *Justis- og beredskapsdepartementet*. S. 35.) har trukket fram sporbarhet som et fjerde prinsipp. Bakgrunnen for dette prinsippet er behovet for å kunne finne ut hva som har skjedd hvis en kompromittering har funnet sted. Da kan det eksempelvis være behov for å vite hvem som har håndtert informasjonen og hvordan den har blitt håndtert. I sikkerhetslovens forskrift om informasjonssikkerhet kommer prinsippet om sporbarhet til uttrykk gjennom tilleggskrav om at sikkerheten i informasjonssystemer skal vurderes ut fra autentisitet, ansvarlighet og tillit. I denne strategien benyttes således sporbarhet som et fjerde prinsipp.

En betydelig del av informasjonen i forsvarssektoren lagres, behandles og sendes i og mellom informasjonssystemer. Sikring av slike systemer krever høy kompetanse og evne til kontinuerlig forbedring. Arbeidet med sikring av informasjonssystemene må derfor gis nødvendig prioritet.

1.1 Rammer

Informasjonssikkerhetsstrategien skal ligge til grunn for all behandling av informasjon og informasjonssystemer i forsvarssektoren. Informasjonssikkerhetsarbeidet skal følges opp gjennom virksomhetens helhetlige styringssystem. Arbeidet med skjermingsverdig informasjon skal primært innrettes etter kravene i sikkerhetsloven og beskyttelsesinstruksen. I likhet med andre forvaltningsorganer må virksomhetene i forsvarssektoren også forholde seg til en rekke øvrige særlover som stiller krav til informasjonssikkerhet, for eksempel personopplysningsloven og arkivloven.[2] Etterlevelse av sikkerhetsloven medfører også forpliktelser som påhviler forsvarssektoren gjennom internasjonale sikkerhetsavtaler, herunder med NATO.

Sikkerhetslovens forskrift om informasjonssikkerhet beskriver tre særskilte målsettinger som skal legges til grunn for arbeidet med sikkerhet i informasjonssystemer og som følgelig skal ivaretas av virksomhetene i forsvarssektoren: Sikker plattform, sikker drift og vedlikehold og sikker håndtering av IKT-hendelser, herunder gjenoppretting.

Forsvarssektorens informasjonssikkerhetsstrategi utfyller gjeldende nasjonale strategi for informasjonssikkerhet, og er tilpasset relevante internasjonale strategier.[3]

1.2 Målgruppe

Informasjonssikkerhetsstrategien gjelder for Forsvarsdepartementet (FD) og underliggende etater.

2. Sentrale utviklingstrekk

Norge er blant verdens mest digitaliserte land, og samfunnet er helt avhengig av digitale systemer for å kunne fungere. Digitale systemer baseres ofte på lange, komplekse verdikjeder. Systemene som utgjør verdikjeden kan eies og kontrolleres av en rekke ulike aktører. Denne oppbyggingen av infrastrukturen kan medføre avhengigheter i og mellom systemene som i dag ikke er kjent. Virksomhetene i forsvarssektoren er avhengig av sivil infrastruktur for å kunne løse sine oppgaver. Dette gjelder hele verdikjeden, fra basistjenester som kraftleveranser, til logistikktjenester og infrastruktur. Denne avhengigheten vil bli forsterket i en alvorlig krisesituasjon eller i væpnet konflikt.

Trusselbildet er komplekst og i stadig forandring. Norge har vært vitne til omfattende sikkerhetspolitiske endringer de siste årene. Rammebetingelser for norsk sikkerhet er forverret, og sårbarhetsbildet blir stadig mer sammensatt.

Globaliseringstrenden gjør det vanskeligere å holde oversikt over leverandørkjeder, mennesker og flyten av varer og tjenester. Konflikter i andre land eller verdensdeler kan få konsekvenser nasjonalt,

[2] I eForvaltningsforskriften forsøkes en rekke av disse kravene sammenstilt. Forskriften er således et godt utgangspunkt for å dekke særlovskravene.
[3] Nasjonal strategi for informasjonssikkerhet (2012), NATO Security Policy C-M(2002)49 Enclosure «F» Information Security, nyeste versjon datert mai 2014, PO(2014) Enhanced NATO Policy in Cyber Defence, 27. mai 2014.

gjennom radikalisering og polarisering. Lojalitets- og tilknytningsforhold hos ansatte blir følgelig mer komplekse.

Kapasitetene som opererer i de tradisjonelle domenene land, sjø, luft og rommet knyttes tettere sammen gjennom digitale systemer. Effektiv samhandling på tvers av de tradisjonelle domenene fordrer derfor velfungerende digitale tjenester og infrastrukturer.

Nettverksoperasjoner blir stadig mer målrettede og teknisk avanserte. De mest avanserte operasjonene utføres av statlige aktører, og dreier seg i hovedsak om kartlegging av infrastruktur og langvarig informasjonsinnhenting. Enkelte aktører innenfor internasjonal industri og næringsliv har også tilgang til offensive kapasiteter, og de bruker avanserte teknikker for å skaffe seg fordeler i forbindelse med anbud og forhandlinger om store kontrakter.[4] Nasjonal sikkerhetsmyndighet (NSM) ser en økende tendens til at trusselaktører angriper underleverandører og mindre virksomheter som kan tenkes å ha tilgang til informasjon om forsvarssektoren.[5]

Etterretningstjenesten (E-tjenesten) peker på det digitale rom som en arena med en betydelig rolle i framtidige kriser og konflikter. Digitale angrep har blitt en integrert del av militære operasjoner. Dette krever styrket evne til å forsvare informasjonssystemer mot digitale angrep i krise og konflikt. Erfaringer fra senere års konflikter viser at en aggressor i en sikkerhetspolitisk krise i økende grad vil forsøke å lamme eller påvirke digital kommunikasjon gjennom elektronisk krigføring og/eller cyberoperasjoner. Moderne kriser stiller derfor særskilte krav om å kunne operere med sterkt redusert støtte fra de digitale systemene.

Samlet sett medfører disse utviklingstrekkene økende risiko for at forsvarssektorens funksjoner, infrastruktur og skjermingsverdige informasjon kan bli rammet av spionasje, sabotasje, terror eller andre alvorlige handlinger. Dette stiller store krav til arbeidet med informasjonssikkerhet i forsvarssektoren.

3. Oppgaver og ansvar

Det overordnede nasjonale ansvaret for IKT-sikkerhet er delt mellom Justis- og beredskapsdepartementet (JD) i sivil sektor og FD i forsvarssektoren.[6] FD er, som ansvarlig departement, overordnet ansvarlig for alt arbeid med informasjonssikkerhet i forsvarssektoren.

FD og etatene i forsvarssektoren har i henhold til ansvarsprinsippet selv ansvar for å ivareta egen informasjonssikkerhet i hele krisespennet. I tillegg til forsvarssektorens ansvar for egen informasjonssikkerhet, har sektoren tverrsektorielle oppgaver innenfor informasjonssikkerhet. NSM er det nasjonale fagmiljøet for IKT-sikkerhet.[7] NSM er også nasjonal varslings- og koordineringsinstans for alvorlige digitale angrep og andre alvorlige IKT-hendelser mot samfunnsviktige virksomheter og informasjon. E-tjenesten har ansvar for vår nasjonale utenlandsetterretning. Etterretning er et viktig bidrag til blant annet arbeidet med tidligvarsling av digitale angrep.

[4] Helhetlig IKT-risikobilde 2015, *Nasjonal sikkerhetsmyndighet* 2015, side 29.
[5] Risiko 2015, Nasjonal sikkerhetsmyndighet
[6] Kgl.res. av 22. mars 2013.
[7] Prop. 1 S (2015-2016), Justis- og beredskapsdepartementet og Instruks for sjef NSM av 5. desember 2014

Sivile myndigheter kan ved særlige behov anmode om bistand fra forsvarssektoren for å ivareta samfunnssikkerheten. Ressursene i forsvarssektoren skal imidlertid først og fremst prioriteres til sikring av sektorens egne informasjonssystemer.

4. Mål for arbeidet med å styrke informasjonssikkerheten

Virksomhetene i forsvarssektoren forvalter betydningsfulle verdier i form av informasjon og digitale tjenester. Disse verdiene må beskyttes for effektivt å kunne motvirke trusler mot rikets selvstendighet, sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Virksomhetene forvalter også informasjon som må sikres av andre årsaker, blant annet informasjon som er omfattet av beskyttelsesinstruksen. Som en konsekvens av dette bruker forsvarssektoren betydelige ressurser på informasjonssikkerhetsarbeid.

Tilstrekkelig sikkerhet kan ikke oppnås ved å benytte tekniske, fysiske eller personellrelaterte virkemidler hver for seg. Virkemidlene må sees i sammenheng. Det er nødvendig at informasjonssikkerhetsarbeidet utføres med en helhetlig tilnærming, og at dette arbeidet integreres i styringen av virksomheten. Virksomhetene må selv vite hvilke verdier de forvalter, hvilket sikringsbehov disse verdiene har og hvilket regelverk virksomheten er underlagt. De må kunne iverksette pålagte tiltak, og for øvrig tiltak som gjenspeiler den totale verdikjeden man ønsker å beskytte.

Selv med en effektiv prioritering mellom de ulike virkemidlene er det urealistisk å oppnå en tilstand med fullstendig sikkerhet. Virksomhetene i forsvarssektoren må derfor ha et bevisst forhold til hjemlet risikovillighet, og systemeier og brukerstedsansvarlig[8] må ha et nødvendig grunnlag for å kunne vurdere akseptabel restrisiko. Økt grad av samhandling, i kombinasjon med avhengighet av sivil infrastruktur, fører til at virksomhetene i forsvarssektoren også har behov for å kjenne samarbeidende virksomheters risikovilje. Dette stiller krav til samarbeid og felles situasjonsforståelse.

For å nå forsvarssektorens målsetting om at informasjonssikkerhetsarbeidet skal bidra til oppgaveløsing i fred, sikkerhetspolitisk krise og væpnet konflikt, må informasjon og informasjons-systemer holdes tilgjengelig på tross av sikkerhetstruende hendelser. Dette stiller krav til virksomhetenes evne til ikke bare å hindre noe i å gå galt, men også til å unngå eskalering av en hendelse og til gjenoppretting av sikker tilstand. Virksomhetene skal tilnærme seg dette arbeidet ved å bygge resiliens. En resilient virksomhet evner å gjenkjenne behovet for respons, agere for å unngå eskalering av situasjonen, opprettholde drift i et endret situasjonsbilde og å lære av hendelsen. Etablering av informasjonssystemer skal følge den samme resiliens-tankegangen. Systemene skal gis et design som gjør dem motstandsdyktige og dynamiske.

To av kjerneverdiene i forsvarssektorens verdigrunnlag er åpenhet og vidsyn. Kravet til åpenhet er først og fremst begrunnet i samfunnets behov for demokratisk kontroll. I forsvarssektoren er det derfor viktig å være tydelig og bevisst på hva virksomhetene kan være åpne om, og hvilken informasjon som må eller bør unntas offentlighet og som derfor har behov for beskyttelse.[9] Vidsyn

[8] Jf. NSMs Veiledning i planlegging av graderte informasjonssystemer, 9. mars 2016. NSM anbefaler ikke å benytte begrepet systemeier for å beskrive roller etter sikkerhetsloven. Systemeier benyttes likevel i denne strategien ettersom eieren av systemene har oppgaver som går ut over sikkerhetsloven.
[9] Jf. offentleglova

vektlegger det helhetlige perspektivet. Denne kjerneverdien understreker viktigheten av tverrfaglig, tverrsektorielt og internasjonalt samarbeid. Samtidig setter vidsynet fagområdene inn i en større ramme. Av dette kan det utledes at kravet til sikkerhet ofte er ett av flere hensyn som skal tas. Verdiene innebærer dermed noen dilemmaer for sikkerhetsområdet som krever refleksjon.

I Nasjonal strategi for informasjonssikkerhet[10] nedfelles fire overordnede mål for arbeidet med informasjonssikkerhet. FD har definert fem mål for informasjonssikkerhet som bygger på disse fire målene, men som er tilpasset sektorens behov.

- God sikkerhetsstyring
- God informasjonskontroll
- Motstandsdyktige informasjonssystemer
- Effektiv håndtering av digitale angrep
- Godt tverrsektorielt samarbeid innen informasjonssikkerhet

Hvert mål er tydeliggjort med en eller flere strategiske prioriteringer. Disse skal tillegges særlig oppmerksomhet, men de gir ikke en uttømmende oversikt over alle områder som må belyses i arbeidet med informasjonssikkerhet.

Mål 1: God sikkerhetsstyring

Sikkerhetsstyring er aktiviteter som gjennomføres for å oppnå og opprettholde et sikkerhetsnivå som er i overensstemmelse med virksomhetens oppdrag, oppgaver og egenart. Effektiv sikkerhetsstyring oppnås gjennom en kombinasjon av forankring, forpliktelse og forståelse.

God sikkerhetsstyring skal oppnås gjennom følgende strategiske prioriteringer:

- **Etablering av et helhetlig styringssystem**
- **Tydelig ledelsesforankring og styrking av sikkerhetskulturen**

Etablering av et helhetlig styringssystem

Det er en forutsetning for en vellykket implementering av forsvarssektorens informasjonssikkerhetsstrategi at sikkerhet inngår i virksomhetenes helhetlige styringssystem. Et styringssystem består av ulike steg som skal sikre en kontinuerlig prosess for å bedre sikkerheten i virksomheten (jf. figur 1). Sårbarhetsreduserende tiltak kan ta tid å etablere, samtidig som risikobildet kan endre seg raskt. Sikkerhetsloven plasserer derfor et betydelig ansvar hos den enkelte virksomhet for å utvikle sikkerhetsarbeidet gjennom risikovurderinger. Sikkerhetsarbeidet skal være risikodrevet, slik at operativ evne[11] sikres, både ved å hensynta dagens lovfestede minimumskrav og ved å arbeide aktivt for å håndtere fremtidig risiko.

[10] Nasjonal strategi for informasjonssikkerhet (2012) etablerte fire overordnede mål for arbeidet med informasjonssikkerhet. 1. Styrket samordning og felles situasjonsforståelse, 2. Robust og sikker IKT-infrastruktur i hele samfunnet, 3. Sterk evne til å håndtere uønskede IKT-hendelser, 4. Høy kompetanse og sikkerhetsbevissthet.

[11] Jf. revidert nasjonalbudsjett 2016 ønsker regjeringen mest mulig operativ evne for bevilgningene. Aktiviteten i sektoren som utføres for sektoren skal følgelig bygge opp under denne målsettingen.

Figur 1: Styringshjul for sikkerhet, hentet fra NSMs «Veileder i sikkerhetsstyring".

Tydelig ledelsesforankring og styrking av sikkerhetskulturen

Sikkerhetsarbeidet må forankres i ledelsen, baseres på en tydelig ansvarsfordeling, og med et kontinuerlig fokus på bevisstgjøring, motivasjon og kompetanseheving. Leder har et særskilt ansvar for å påse at sikkerhetsorganisasjonen er dimensjonert for å kunne ivareta sikkerhetsarbeidet.

Virksomhetene i forsvarssektoren skal forstå trusselbildet. Samtidig skal virksomhetene ha kunnskap om verdiene i sin virksomhet som har betydning for Forsvarets operative evne og om sårbarheter som kan utnyttes for å ramme disse verdiene. Dette krever at den enkelte virksomhetsleder setter sikkerhet på agendaen, og at sikkerhetsarbeidet anses sentralt for å sikre den operative evnen.

Sikkerhetstiltakene må balanseres mellom tekniske, fysiske, organisatoriske og personellrelaterte tiltak. Det gir begrenset effekt å bygge omfattende tekniske sikkerhetsmekanismer dersom de digitale systemene, på grunn av mangel på tilgjengelighet eller funksjonalitet, ikke er egnet til å formidle rettidig og pålitelig informasjon. Det er heller ikke hensiktsmessig å legge alle ressursene i digital sikring av informasjonssystemene uten å sikre informasjon, personell og prosesser i egen organisasjon, og mellom egen og andre organisasjoner.

Virksomhetene i forsvarssektoren skal ha en god sikkerhetskultur og kontinuerlig jobbe med å forbedre denne. Sikkerhetskultur defineres som summen av kunnskap, motivasjon, holdninger og adferd. Sikkerhetskulturen skapes i virksomhetsledelsen, og ledere i sektoren skal derfor måles på sikkerhet. Det påhviler også hver medarbeider et særskilt ansvar for å bidra til en styrket sikkerhetskultur.

Kunnskapen skal inkludere sikkerhetskompetanse, herunder teknologikompetanse, leder- og medarbeideradferd og evne til å bidra til en god sikkerhetskultur. Som et verktøy for blant annet kompetanseutvikling skal arbeidet innen holdninger, etikk og ledelse (HEL) vektlegges. HEL-arbeidet skal inkludere dilemmatrening innen sikkerhet.

Mål 2: God informasjonskontroll

Virksomhetene i forsvarssektoren skal sikre informasjon i henhold til de krav som stilles for det aktuelle sikkerhetsgraderingsnivået. Tilgang til graderte informasjonssystemer og gradert

informasjon skal kun gis til personell med tilstrekkelig klarering og autorisasjon. I tillegg skal virksomhetene ha et bevisst forhold til informasjon som er skjermingsverdig av andre grunner enn etter sikkerhetsloven og beskyttelsesinstruksen. Dette gjelder blant annet informasjon som omfattes av arkivloven, regnskapsloven eller personopplysningsloven. Det er informasjonsutsteders ansvar å vurdere hvilket beskyttelsesbehov informasjon har. Avhengig av behov stilles det spesifikke krav til bl.a. merking og oppbevaring. Forsvarssektoren skal styrke sin kontroll med skjermingsverdig informasjon, og bidra til større åpenhet om informasjon som ikke krever skjerming.

God informasjonskontroll skal oppnås gjennom følgende strategiske prioriteringer:

- **Styrket bevissthet om skjermingsbehov**
- **Økt bruk av krypto**

Styrket bevissthet om skjermingsbehov

Usikkerhet rundt det reelle graderingsbehovet, i tillegg til holdninger og sedvane i organisasjonen, kan bidra til at informasjon graderes feil. I mange tilfeller fører dette til at informasjonen gis en unødvendig høy gradering. Det er ressurskrevende å verne om skjermingsverdig informasjon, og bruk av unødvendig høye graderinger vil følgelig resultere i unødig ressursbruk. Manglende kommunikasjonsmuligheter for gradert informasjon har motsatt effekt, og bidrar til at informasjon som burde vært gradert unntas gradering, eller behandles på et for lavt graderingsnivå. Forsvarssektoren skal redusere problemet med feilgradering av informasjon. Sektoren skal prioritere fortløpende å ned- og avgradere dokumenter. Informasjon som avgraderes, eksempelvis i forbindelse med behandling av en innsynsbegjæring, skal være korrekt avgradert.[12] Det skal ikke være tvil om at dokumentet er avgradert, og at avgraderingen er foretatt av kompetent myndighet.

I en operativ kontekst vil det produseres informasjon som har en kortsiktig, taktisk verdi. Skjermingsbehovet for slik informasjon vil kunne avta raskere enn for informasjon av strategisk betydning. Unødig langvarig skjerming av informasjon er kostbart. Forsvarssektoren skal derfor vurdere løsninger som på en bedre måte kan ivareta de kortsiktige behovene for skjerming av taktisk informasjon, samtidig som lovpålagte krav ivaretas.

Økt bruk av krypto

E-post som sendes mellom ugraderte IKT-systemer formidles i mange tilfeller åpent og ukryptert over internett. Virksomhetene i forsvarssektoren skal ha et bevisst forhold til sikring av informasjon. Ekstern kommunikasjon av sensitiv informasjon skal krypteres. Også digitalt lagret informasjon skal sikres ved hjelp av kryptering. Forsvarssektoren skal bidra til en helhetlig nasjonal tilnærming til nye kryptoløsninger.

Mål 3: Motstandsdyktige informasjonssystemer

Ved sikkerhetspolitiske kriser eller i væpnet konflikt vil forsvarssektoren kunne utsettes for forsøk på å påvirke kommunikasjon og våpensystemer. De senere års trussel- og sårbarhetsbilde indikerer at det ikke vil være mulig å holde en motstander utenfor sektorens systemer i en sikkerhetspolitisk krise eller i væpnet konflikt. Skallsikring i form av barrierer er ikke tilstrekkelig. For forsvarssektoren er det viktig å kunne opprettholde tilgjengelighet til systemer og informasjon på tross av IKT-hendelser.

[12] Forskrift om informasjonssikkerhet §§ 4-5 og 4-6.

Systemene må også kunne konfigureres til å tilpasse informasjonsflyten til endrede forutsetninger, både under og etter ekstraordinære påkjenninger. Forsvarssektoren skal forvalte sine systemer i tråd med utviklingen i både teknologi og i trusselbilde.

Motstandsdyktighet skal oppnås gjennom følgende strategiske prioriteringer:

- **Robuste og dynamiske systemer**
- **Kontinuerlig forbedring**
- **Redusert antall ugraderte systemer**

Robuste og dynamiske systemer

Forsvarssektoren skal fokusere på tilpasningsdyktighet og evne til å opprettholde tjenester under uforutsette hendelser. Systemene skal kjennetegnes ved både robusthet og redundans, men også ved tilstrekkelig fleksibilitet til å kunne tilpasse seg hurtige endringer i trusselbildet. Systemenes og informasjonens integritet må også kunne kontrolleres under pågående uforutsette hendelser.

Ved design av kritiske operative systemer, operativt støttende systemer og systemer for forvaltning skal det innarbeides tilstrekkelig robusthet, redundans og tilpasningsevne til å kunne sikre tilgjengelighet og gjenopprettingsevne i kritiske situasjoner. Sektorens systemer skal i nødvendig utstrekning kunne motvirke effekten av tilsiktede og utilsiktede uforutsette hendelser.

Kontinuerlig forbedring

Gjennom sin levetid tilpasses mange systemer til å ivareta oppgaver de ikke var tiltenkt da de ble utviklet. Det betyr at arbeidet med herding og videreutvikling av anskaffede systemer må ha et kontinuerlig fokus. Det er systemeiers ansvar å avsette tilstrekkelige ressurser til kontinuerlig forbedring, og til å påse at kompetansen til personellet som forvalter systemene oppdateres i takt med utviklingen av systemene.

Redusert antall ugraderte systemer

Forsvaret har behov for effektivt samvirke med eksterne aktører, herunder industri og tjenesteleverandører. Fraværet av forvaltet IKT som er egnet til formålet, resulterer i at det etableres lokale ugraderte løsninger som ikke er underlagt sentral forvaltning. Det er en sikkerhetsmessig risiko forbundet med manglende kontroll og oversikt over ugraderte IKT-systemer og -infrastruktur i Forsvaret. Antallet ugraderte nett og IKT-plattformer skal derfor reduseres og underlegges bedre kontroll.

Mål 4: Effektiv håndtering av digitale angrep

Håndtering av digitale angrep omfatter både håndtering av sikkerhetstruende hendelser og gjenoppretting av normaltilstand. Læringen fra slike hendelser skal nyttiggjøres, slik at man oppnår kontinuerlig forbedring av systemer og rutiner. Sikkerhetstruende hendelser håndteres best når rutiner for håndteringen er inkludert i virksomhetens styringssystem.

Effektiv håndtering av digitale angrep skal oppnås gjennom følgende strategiske prioriteringer:

- **Økt sporbarhet**
- **Øving på hendelseshåndtering og bortfall av kommunikasjon**

Økt sporbarhet

Det legges ned omfattende innsats for å avdekke og håndtere digitale angrep mot forsvarssektorens informasjon og informasjonssystemer. Egeninnsats og et omfattende nasjonalt og internasjonalt samarbeid innen etterretning bidrar til å gi oss evne til å spore uønsket aktivitet i og utenfor egne IKT-systemer. Forsvarssektoren skal gjennom styrket samarbeid og kompetanse øke evnen til hendelseshåndtering.

Sporbarhet i egne systemer er en forutsetning for å kunne avdekke hva som har skjedd ved en informasjonslekkasje og hvilken informasjon som eventuelt er tapt. Revisjonen av sikkerhetsloven 8. juni 2016 gir hjemmel for en mer omfattende logging av aktiviteten i og mellom informasjonssystemer som er underlagt loven.[13] Dette gir virksomhetene en bedre mulighet til å oppdage og spore uønsket aktivitet. Basert på det nye hjemmelsgrunnlaget skal virksomhetene i forsvarssektoren implementere hensiktsmessig logging i informasjonssystemene.

Øving på hendelseshåndtering og bortfall av kommunikasjon

På tross av en effektiv hendelseshåndtering vil virksomhetene måtte forberede seg på forstyrrelser i systemene. Det er derfor vesentlig at det etableres kompenserende tiltak for å opprettholde evnen til kommunikasjon mellom særlig viktige lokasjoner ved bortfall av ordinære kommunikasjons-løsninger. Bortfall av kommunikasjonsløsninger skal øves.

Mål 5: Godt tverrsektorielt samarbeid innenfor informasjonssikkerhet

Sårbarheter som oppstår i én sektor kan gi konsekvenser i andre sektorer. Forsvarssektoren er avhengig av en rekke leveranser fra det sivile samfunn, blant annet innen kraft, forsyning og infrastruktur. For eksempel er den underliggende infrastrukturen som benyttes av Forsvaret delvis eid av private aktører. Et velfungerende tverrsektorielt samarbeid er derfor viktig for å oppnå en god samlet sikkerhetstilstand.

Virksomhetene i forsvarssektoren skal bidra til styrket tverrsektorielt samarbeid om informasjons-sikkerhet gjennom følgende strategiske prioriteringer:

- **Kartlegge avhengigheter av sivil infrastruktur**
- **Bidra til økt sikkerhetsforståelse i leverandørkjeden**
- **Styrke samarbeidet med relevante samarbeidspartnere**

Kartlegge avhengigheter av sivil infrastruktur

Sammenhengen mellom ulike systemer er kompleks og uoversiktlig. Kontroll over egne avhengigheter er derfor en forutsetning for oversikt over egen sikkerhet. Norge vil i de øvre delene av krisespennet kunne være vert for styrker fra samarbeidende nasjoner. Avhengigheter vil således også kunne påvirke våre alliertes sikkerhet. Virksomhetene skal ha oversikt over avhengigheter av sivil infrastruktur, og skal sikre tilstrekkelig oppetid gjennom avtaler eller samarbeid.

Bidra til økt sikkerhetsforståelse i leverandørkjeden

Når stadig flere IKT-systemer kobles sammen på tvers av sektorer og landegrenser og til internett, øker også sannsynligheten for svake ledd som ikke er tilstrekkelig sikret. Utenlandske etterretningsorganisasjoner legger ned betydelige ressurser for å utnytte slike svake ledd, i den

[13] Jf. Lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste. Sist endret 8. juni 2016. Ny § 13a Sikkerhetsmessig overvåking av godkjente informasjonssystemer.

hensikt å få tilgang til forsvarshemmeligheter og bedriftssensitiv informasjon. Det er en økende tendens til at trusselaktørene søker å hente informasjon fra leverandører som er direkte eller indirekte tilknyttet myndighetene og forsvarsindustrien. I tillegg til å sikre egne systemer, er virksomhetene i forsvarssektoren avhengig av at leverandører og underleverandører evner å beskytte slik informasjon, uavhengig av om den er sikkerhetsgradert eller ikke. NSM vurderer at utenforståendes utnyttelse av mangelfull risikoforståelse og sikkerhet hos underleverandører er et økende nasjonalt problem. Forsvarssektoren skal derfor bidra til en god situasjonsforståelse i leverandørkjeden.

Styrke samarbeidet med relevante samarbeidspartnere

Forsvarssektoren har gjennom E-tjenesten og NSM et godt grunnlag for å kunne vurdere trusler og sårbarheter i informasjonssystemene. For å kunne iverksette effektive tverrsektorielle mottiltak, er sektoren avhengig av at også sivile aktører besitter den samme situasjonsforståelsen og ivaretar sikkerheten på en forsvarlig måte. Virksomhetene i forsvarssektoren skal gjennom informasjonsdeling og rapportering bidra til å øke bevisstheten rundt trusler og sårbarheter i samfunnet.

CYFOR utdanner årlig omlag 40 ingeniører med kompetanse innen drift og forvaltning av Forsvarets IKT-systemer og infrastruktur. Dette gjøres i tett samarbeid med relevante sivile utdannings-institusjoner. Ingeniører utdannet av CYFOR har imidlertid ikke en kompetanseprofil som dekker hele forsvarssektorens behov. Dette gjelder blant annet innen analyse, håndtering av IKT-hendelser og kryptografi. For å dekke sektorens behov for kompetanse skal etatene søke samarbeid med sivile utdanningsinstitusjoner og nære allierte, i tråd med Mld. St. 14 (2012-2013)

5. Implementering

Denne strategien operasjonaliseres gjennom iverksettingsbrev for forsvarssektoren. Økonomiske og administrative konsekvenser av tiltak som følger av denne strategien behandles i de ordinære budsjettprosessene.