NASJONAL
SIKKERHETSMYNDIGHET

RISIKO 2019

Krafttak for et sikrere Norge

NSMs rapport «Risiko 2019» er én av fire trussel- og risikovurderinger som utgis årlig. De øvrige tre utgis av Etterretningstjenesten, Politiets sikkerhetstjeneste og Direktoratet for samfunnssikkerhet og beredskap.

Nasjonal sikkerhetsmyndighet (NSM) er Norges fagmyndighet for forebyggende nasjonal sikkerhet. NSM gir råd om og fører tilsyn med blant annet sikring av informasjon, objekter og infrastruktur av nasjonal betydning. Videre har NSM et nasjonalt ansvar for å detektere, varsle og koordinere håndtering av alvorlige IKT-angrep. I rapporten «Risiko 2019» vurderer NSM risikoen for at samfunnet skal rammes av spionasje, sabotasje, terror og andre alvorlige handlinger. Vurderingen utgis i første kvartal.

Etterretningstjenesten (E-tjenesten) er Norges utenlandsetterretningstjeneste. Tjenesten er underlagt forsvarssjefen, men arbeidet er ikke avgrenset til militære problemstillinger. E-tjenestens hovedoppgaver er å varsle om ytre trusler mot Norge og prioriterte norske interesser, støtte Forsvaret og forsvarsallianser Norge deltar i, samt understøtte politiske beslutningsprosesser med informasjon av spesiell interesse for norsk utenriks-, sikkerhets- og forsvarspolitikk. «Fokus 2019» gir E-tjenesten sin analyse av status og forventet utvikling innenfor geografiske og tematiske områder som tjenesten vurderer som særlig relevant for norsk sikkerhet og nasjonale interesser. Etterretningsvurderingen har en tidshorisont på ett år, og utgis i første kvartal.

Politiets sikkerhetstjeneste (PST) er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste. PSTs hovedoppgave er å forebygge og etterforske alvorlig kriminalitet mot nasjonens sikkerhet. PSTs årlige trusselvurdering er en analyse av forventet utvikling innenfor PSTs hovedansvarsområder.

Direktoratet for samfunnssikkerhet og beredskap (DSB) skal ha oversikt over risiko og sårbarhet i samfunnet. DSB har utgitt scenarioanalyser siden 2011. Analysene omhandler risiko knyttet til katastrofale hendelser som kan ramme det norske samfunnet og som det bør være forberedt på å møte. Analysene omfatter både naturhendelser, store ulykker og tilsiktede handlinger. De har en lengre tidshorisont enn de årlige vurderingene til de øvrige tre etatene.

Innhold

RISIKO 2019

Design: Redink
Trykk og distribusjon: RK grafisk

Forord

2019 er et merkeår for vårt nasjonale sikkerhetsarbeid. 1. januar trådte ny sikkerhetslov i kraft, et verktøy som vil gjøre det mulig å treffe nødvendige tiltak for å styrke og modernisere nasjonal sikkerhet.

Den nye loven gir hvert departement et tydelig ansvar for å identifisere og holde oversikt over hvilke verdier som bør beskyttes innenfor sitt ansvarsområde. For oss i Nasjonal sikkerhetsmyndighet (NSM) betyr loven nye oppgaver og et enda større ansvar, bl.a. med å forvalte og fordele informasjon om trusler og sårbarheter som påvirker nasjonal sikkerhet. Vi bruker mye ressurser i år på å lage veiledere og gi råd om hvordan sikkerhetsarbeidet bør innrettes med nytt lovgrunnlag og i en ny tid.

Samtidig foregår det flere, gode initiativer som hever sikkerheten, både på nasjonalt plan, i de enkelte sektorene og i virksomhetene, og både utenfor og innenfor sikkerhetslovens område. NSM opplever at særlig IKT-sikkerhet står stadig høyere på agendaen blant norske ledere. Nye nasjonale sentre, som Nasjonalt cyberkrimsenter under Kripos og NSMs satsning på et Nasjonalt cybersikkerhetssenter, vil gjøre oss bedre rustet til å møte et bredt spekter av digitale trusler gjennom større grad av tverrsektorielt og offentlig-privat samarbeid.

Trusselbildet mot norske verdier er dynamisk, og sammen med den samfunnsmessige og teknologiske utviklingen skjer endringer så raskt at mottiltakene ikke henger med. Hos NSM NorCERT går alarmen mange ganger daglig, og vi ser stadig mer komplekse og omfattende angrep.

NSM oppfordrer i dette merkeåret til et nasjonalt krafttak for sikkerhet, der samhandling, informasjonsutveksling og offentlig-privat samarbeid står sentralt. Den nye sikkerhetsloven gir myndighetene mulighet til å styre risikoen bedre på nasjonalt nivå, gjennom å identifisere viktige funksjoner og utpeke virksomheter. For at nasjonalt sikkerhetsarbeid skal få full effekt, er det avgjørende at den enkelte virksomheten kjenner sin verdi og sin funksjon i det store samfunnsmaskineriet. Hva har din virksomhet som bør beskyttes, ikke bare for bunnlinjas del, men også ut fra hvilken verdi den utgjør for samfunnet?

Foto: Cicilie S. Andersen

Kjetil Nilsen
Direktør NSM

Sammendrag

Samfunnet vårt er i stadig endring. Kommersiell verdiskaping og teknologiutvikling fornyer og forbedrer måten vi lever og arbeider på. Samtidig vil globale faktorer der vi har svært begrenset mulighet for påvirkning, også virke inn på utviklingen her hjemme.

Den økende digitaliseringen er et tveegget sverd. Utviklingen av teknologi skaper på den ene siden rom for innovasjon og effektivisering. På den andre siden oppstår nye sårbarheter, og den totale digitale angrepsflaten øker. NSM erfarer stadig mer avanserte og effektive nettverksoperasjoner rettet mot norske virksomheter. Dette utgjør en betydelig risiko for viktige samfunnsfunksjoner.

Norske myndigheter innfører stadig nye risikoreduserende tiltak for å møte det komplekse trussel- og risikobildet vi står overfor. For å kunne styre risikoen bedre for våre viktigste funksjoner trådte en ny og moderne sikkerhetslov i kraft ved inngangen til 2019. Behovet for ny lov begrunnes spesielt i teknologiutvikling og globalisering, der virksomheter og funksjoner på tvers av samfunnet er avhengige av hverandre i større grad enn før.

Det er innført en rekke tiltak for å styrke nasjonalt cybersikkerhetsarbeid, i en tid der digitale angrep utgjør en omfattende utfordring. Det opprettes nye nasjonale sentre for å kraftsamle om digital sikkerhet. NSM registrerer også at det gjøres mye bra og riktig sikkerhetsarbeid i norske virksomheter, og spesielt IKT-sikkerhet kommer stadig høyere på norske lederes dagsorden. NSM vil fremheve næringslivet som en sentral medspiller i sikkerhetsarbeidet, både i kraft av å forvalte viktige samfunnsfunksjoner og som leverandør til offentlige etater. Ved å redusere antall klareringsmyndigheter til én sivil og én for forsvarssektoren samles og styrkes nasjonal personellsikkerhets- og sikkerhetsklareringskompetanse. Det gjøres også grep for å styrke sikkerhetskompetansen i stort, både gjennom økt fokus på høyere utdanning innen sikkerhet og gjennom kursvirksomhet og veiledning.

Ved å se verdiene vi ønsker å beskytte i sammenheng med sårbarheter i norske virksomheter, trusselbildet mot norske interesser samt ytre forhold og utviklingstrekk, har NSM identifisert seks risikofaktorer. Disse faktorene må håndteres i det forebyggende nasjonale sikkerhetsarbeidet i årene som kommer.

Seks risikofaktorer

1. Et ufullstendig **risikobilde** gjør det vanskelig å sikre samfunnet med de riktige tiltakene. NSM erfarer at for mange virksomheter fortsatt har mangelfull oversikt over egne sårbarheter og eget risikobilde. Vi må vite hva vi står overfor, både på virksomhetsnivå og på myndighetsnivå.

2. For svak **sikkerhetsstyring** i det daglige fører til at både personell-sikkerhetsmessige, fysiske og digitale tiltak ikke blir sett i sammenheng og fulgt opp i nødvendig grad.

3. Svakheter eller mangler i virksomhetens **personellsikkerhetsarbeid** kan gjøre det lettere for innsidere å operere uoppdaget. En innsider kan effektivt undergrave andre sikkerhetsbarrierer, slik som sikring av IKT-nettverk og fysisk sikring av bygninger.

4. Funksjoner som i dag ikke er heldigitaliserte, eller tilgjengelige via en digital inngangsport, vil i stor grad bli det i fremtiden. Utilstrekkelig sikring av samfunnsviktig **informasjon og informasjonssystemer** utgjør risiko for at trusselaktører kan få tilgang til langt flere av våre verdier fremover.

5. Det er forventet at flere **skjermingsverdige objekter og infrastrukturer** vil bli pekt ut som følge av ny sikkerhetslov. Mangler i kartlegging av avhengigheter og dermed manglende helhetlig sikring av objekter og infrastrukturer øker risikoen for at trusselaktører kan finne sårbarheter i, og om ønskelig, sette viktige samfunnsfunksjoner ut av spill.

6. **Næringslivet** vil i enda større grad levere tjenester og utstyr til viktige samfunnsfunksjoner i fremtiden. Det er sentralt at man på både offentlig og privat side vurderer og dimensjonerer risikoreduserende tiltak med dette som bakteppe.

Risikofaktorene henger sammen og forsterker hverandre. For eksempel blir innsideren en langt større trussel i en virksomhet der nettverkene ikke er godt segregert, godt tilgangsstyrt og beskyttet med logging. Risikobasert sikkerhetsstyring er verktøyet som skal løse hele spekteret av slike utfordringer.

1

Risikobildet

Risikobildet er NSMs vurdering av hvordan sårbarheter, trusler og andre utviklingstrekk påvirker risikoen for viktige samfunnsfunksjoner og -verdier i tiden fremover. Vi kartlegger sikkerhetstilstanden med bakgrunn i sårbarhetsfunn både innenfor og utenfor sikkerhetslovens virkeområde.

Verdier

For å ivareta stats- og samfunnssikkerhet er det en rekke viktige funksjoner som må sikres. Våre nasjonale sikkerhetsinteresser vil være styrende for hvilke funksjoner vi er avhengige av at fungerer. Skillet mellom stats- og samfunnssikkerhet er i stadig endring, og overgangen er mer glidende enn for bare få år siden.

Verdiene vi skal beskytte i henhold til sikkerhetsloven er våre aller mest sentrale samfunnsfunksjoner. Departementene er ansvarlige for å identifisere disse *grunnleggende nasjonale funksjonene*. NSM forventer at departementene vil se behov for å beskytte flere objekter, infrastrukturer og informasjonssystemer som følge av den nye sikkerhetslovens utvidede virkeområde og endrede systematikk – og altså identifisere disse som skjermingsverdige.

Her følger noen eksempler på områder der våre nasjonale verdier er i endring.

Territorielle verdier: En isfri Nordøst-passasje kan aktualisere politiske og juridiske spørsmål om rettigheter i Nordområdene. Norske olje- og gass-forekomster forventes å være strategiske ressurser helt frem mot år 2040.

Verdien av informasjon: Informasjonen i samfunnet øker kraftig både i volum og verdi. Store aktører som Google og Facebook sitter på mye informasjon om nordmenn og norske forhold, og denne informasjonsinnsamlingen vil øke. Norske virksomheter, også offentlige, bruker kunstig intelligens-systemer levert og driftet av utenlandske selskaper, ofte plassert i utlandet. Når denne typen virksomheter har tilgang til og kan sammenfatte data fra flere kilder, vil de kunne foredle disse dataene i en helt annen grad enn en norsk, offentlig virksomhet som kun skal ha tilgang på sine egne data. Ved lokalisering i utlandet kan disse dataene bli underlagt utenlandsk lovverk.

Forsvarssystemer: Fremtidens forsvars-systemer er mer automatiserte, mer kostbare og i enda større grad utviklet i sivilt-militært samarbeid.

Infrastruktur: Tilgangen til ikke-digitale verdier vil i større grad styres digitalt. All infrastruktur, inkludert kraft, blir derfor mer avhengig av elektronisk kommunikasjon (ekom), som igjen er avhengig av tilgang på kraft. Et eksempel i denne sammenhengen er utviklingen av det norske 5G-nettet, som vil danne grunnlaget for nye tjenester og funksjoner og skape nye avhengigheter.

Næring og teknologi: Det globale finansielle systemet blir mer sammen-koblet og derfor mer sårbart mot angrep fra både stater og ikke-statlige aktører. Det blir stadig viktigere å beskytte kunn-skap for å sikre teknologiske fremskritt og beholde det teknologiske overtaket.

Trusler

Gjennom samarbeidet med Etterretningstjenesten og PST ser NSM at truslene Norge står overfor og trusselaktørenes interesser er dynamiske og rettet mot et bredt spekter av sektorer og virksomheter. Aktørenes intensjon og kapasitet, sammen med deres måte å operere på, er dimensjonerende for hvordan vi som nasjon, virksomhet og individ må sikre våre verdier. NSM registrerer gjennom varslingssystemet for digital infrastruktur (VDI) og FCKS-samarbeidet[1] at norske virksomheter daglig blir utsatt for digitale hendelser.

Hendelsestall fra NSM NorCERT i 2018

NSM NorCERT registrerte i 2018 ca. 20 000 alarmer om IKT-hendelser. Av disse var i underkant av 5000 såkalt manuelt bearbeidede saker, dvs. at hendelsen ble videre undersøkt.

Et fåtall av disse kategoriseres som alvorlige hendelser, det vil si digitale innbrudd eller annen uønsket aktivitet mot virksomheter som understøtter kritisk infrastruktur eller andre viktige samfunnsfunksjoner. Dette antallet har vært relativt jevnt de siste årene, men NSM vurderer at de mest alvorlige sakene nå er mer omfattende og komplekse. Håndtering og opprydding blir mer krevende og opptar mer ressurser enn tidligere.

[1] Felles cyberkoordineringssenter består av representanter fra NSM, Etterretningstjenesten, PST og Kripos og koordinerer partenes håndtering av IKT-sikkerhetshendelser.

ETTERRETNINGSTRUSSELEN
Etterretningstrusselen mot Norge er vedvarende og kjennetegnes særlig av nettverksoperasjoner og forsøk på å rekruttere personer i viktige norske virksomheter. Både offentlige og private virksomheter som forvalter eller understøtter grunnleggende nasjonale funksjoner, kritisk infrastruktur, forskning eller høyteknologi er potensielle mål for fremmede staters etterretningsvirksomhet.

NETTVERKSOPERASJONER
NSM ser stadig avanserte og målrettede nettverksoperasjoner mot både private og offentlige virksomheter. Kombinasjonen av åpent tilgjengelig skadevare og utdaterte og sårbare systemer har ved flere tilfeller ledet til at norske virksomheters informasjonssystemer har blitt kompromittert.

ANDRE DIGITALE TRUSLER
NSM ser regelmessig tilfeller av mindre avanserte hendelser, som ofte er motivert av økonomisk vinning. Slike hendelser kan potensielt få alvorlige konsekvenser for viktige samfunnsfunksjoner. Eksempler er ulike former for svindel, kryptolåsing, utvinning av kryptovaluta og opportunistiske angrep.

PÅVIRKNINGSOPERASJONER
Både private og offentlige virksomheter kan bli utsatt for påvirkningsoperasjoner. Dette innebærer at en aktør gjennom fordekte virkemidler påvirker og styrer beslutninger i en spesifikk retning. Slike operasjoner kan for eksempel gjøres ved bruk av sosiale medier for å svekke tillit til en konkret virksomhet, institusjon eller enkeltsak.

INNSIDERTRUSSELEN
Enkeltindivider kan bli rekruttert av trusselaktører for å fungere som innsidere. Individer vil også på eget initiativ kunne agere som en innsider og skade en virksomhets verdier.

STRATEGISKE INVESTERINGER OG OPPKJØP
NSM er bekymret for at enkelte stater benytter investeringer og oppkjøp som strategiske virkemidler for å oppnå tilgang til informasjon, teknologi, beslutninger og naturressurser.

KARTLEGGING
Fremmede etterretningstjenester driver kartleggingsaktivitet mot norske mål, rettet mot enkeltindivider og virksomheter for å avdekke funksjoner og sårbarheter innen norsk kritisk infrastruktur, krisehåndtering og sikkerhet og beredskap. Mye av kartleggingen vil utføres ved hjelp av teknisk overvåking, deriblant droner.

JAMMING
Jamming representerer en utfordring for norsk og alliert øvingsaktivitet, og mot sivil luftfart i fredstid. Der sivil luftfart er rammet, kan også viktige funksjoner som redningstjeneste og beredskapstjenester bli satt ut av spill. I forbindelse med militærøvelsen Trident Juncture høsten 2018 ble det registrert flere tilfeller av GPS-jamming som påvirket norsk og alliert luftfart.

TERRORTRUSSELEN
Vold utført av islamistiske ekstremister utgjør fortsatt den største terrortrusselen mot Norge. Til tross for at PST rapporterer om et økt antall høyreekstreme, vurderes det som lite sannsynlig at denne gruppen vil gjennomføre terrorangrap i Norge i 2019.

Sårbarheter og håndtering av risiko

Forebyggende sikkerhetsarbeid handler i stor grad om å håndtere risiko gjennom tiltak som reduserer sårbarheter. Etter ny sikkerhetslov skal en risikovurdering ligge til grunn for sikringen av virksomhetens skjermingsverdige verdier.

Nødvendige tiltak må identifiseres for å oppnå et forsvarlig sikkerhetsnivå. Helhetlig sikring oppnås ved at ulike tiltak virker sammen; for eksempel digitale tiltak sammen med personellmessige og fysiske sikkerhetstiltak. Prinsippet om helhetlig sikring er avgjørende uavhengig av om virksomheten er underlagt sikkerhetsloven eller ikke.

I likhet med andre styringsverktøy er sikkerhetsstyring et nødvendig virkemiddel for arbeid med kontinuerlig forbedring av sikkerheten.

Sikkerhetsstyring er avgjørende for at riktig tiltak identifiseres og iverksettes og for å sørge for helhetlig sikring. Svakheter i sikkerhetsstyringen medfører at personellmessige, digitale og fysiske sårbarheter forblir åpne.

Her følger eksempler på sårbarheter NSM har sett det siste året:

Digitale sårbarheter

- Manglende oversikt over nettverkets oppbygging
- Tap av kontroll over data og funksjonalitet på bakgrunn av inngått samarbeid med underleverandører eller andre virksomheter
- Bruk av standardpassord og gjenbruk av passord
- Bruk av gamle operativsystemer og applikasjoner med kjente sårbarheter
- Manglende blokkering av uautoriserte programmer
- E-post og internetteksponerte servere som har fungert som digital angrepsvektor

Sårbarheter i virksomheters sikkerhetsstyring

- Utilstrekkelig ledelsesforankring av sikringsmål
- Manglende risikovurdering som grunnlag for tiltak
- Mangelfull risikoerkjennelse
- Mangler i permanent grunnsikring og balansen mellom ulike sikringstiltak i viktige virksomheter
- Manglende kartlegging av avhengigheter til andre virksomheter
- Mangelfull operasjonalisering av identifiserte sikkerhetstiltak
- Utilstrekkelig sikkerhetskompetanse

Personellmessige sårbarheter

- Utilstrekkelig evne til å oppdage og håndtere potensielle innsidere
- For svak sikkerhetsmessig oppfølging av ansatte i det daglige
- Mangelfull sikkerhetsmessig opplæring av personell

Fysiske sårbarheter

- Mangelfull sjekk av ID- og adgangskort.
- Bruk av adgangskort med dårlig sikkerhetsteknologi
- Mangelfull sikring mot droner
- Dører og porter som holdes åpne for personer uten legitim adgang (muliggjør såkalt tailgating)

NSM ser at IKT-hendelser rammer store offentlige virksomheter med uoversiktlig og kompleks digital infrastruktur, der det nærmest er umulig å holde oversikt over sårbarheter og avhengigheter.

Risikofaktorer

Et bilde av risikoen Norge står overfor tegnes når vi ser på verdiene våre, truslene som tiltrekkes av disse og sårbarhetene som finnes i beskyttelsen av verdiene. Risikoen håndteres ved å iverksette tiltak for å lukke sårbarhetene. For noen tiltak kan det ta lang tid før ønsket effekt oppnås. Det er viktig at vi løfter blikket og undersøker hvilke samfunnsmessige og teknologiske utviklingstrekk som påvirker risikobildet. NSM har derfor sammenstilt **samfunnsmessige og teknologiske utviklingstrekk** som påvirker risikobildet i fremtiden:

1. Tilgang til naturressurser
2. Forholdet mellom stater – skifte i de globale maktforholdene
3. Migrasjon
4. Forholdet mellom stat og borger
5. Akkumulering av informasjon i nettverk
6. Ny teknologi og tilgang til teknologi
7. Fremtidens forsvarsteknologi
8. Nye domener for krigføring

I dette ligger kunnskapen om hvilke funksjoner som vil være verdifulle for oss i fremtiden, trusselaktørers mulighetsrom og, ikke minst, sårbarhetene som oppstår i fremtidens viktige samfunnsfunksjoner.

Under vurderer NSM risikofaktorer som har betydning for sikringen av grunnleggende nasjonale funksjoner og nasjonale sikkerhetsinteresser i fremtiden.

Risikobilde og risikoforståelse

Departementene har ansvaret for det forebyggende sikkerhetsarbeidet innenfor sitt myndighetsområde. Det betyr at de må identifisere hvilke verdier som må sikres, kjenne til risiko og risikoreduserende tiltak og avhengigheter innen sektoren og til andre sektorer. Virksomhetene har ansvaret for å sikre sine verdier som har betydning for samfunnet. Samspillet mellom myndigheter og virksomheter som forvalter våre skjermingsverdige verdier er derfor viktig for nasjonal sikkerhet.

Volumet og verdien av informasjon fortsetter å øke som følge av at samfunnsprosesser kobles sammen og digitaliseres. NSM ser at IKT-hendelser rammer store offentlige virksomheter med uoversiktlig og kompleks digital infrastruktur, der det nærmest er umulig å holde oversikt over sårbarheter og avhengigheter. Teknologiutviklingen går så raskt at det utfordrer myndighetenes evne til å tilpasse seg og implementere nødvendig regulering og andre tiltak.

NSM, Etterretningstjenesten og PST ser vedvarende høy etterretningsaktivitet mot Norge, fokusert på å skaffe informasjon om politiske og militære mål. Industrispionasje utgjør også en utfordring.

Med dette som bakteppe er det sentralt for norske virksomheter å ha oversikt over egne sårbarheter og

NSM har gjennom en årrekke pekt på at mangelfull sikkerhetsstyring er en av de viktigste årsakene til utilfredsstillende sikkerhetstilstand.

egen risiko. Mangelfull risikoforståelse vil gjøre at sikkerhetsbarrierer etableres på feilaktige premisser eller ikke i det hele tatt. Dette reduserer virksomhetens sikkerhetsnivå og øker sannsynligheten for at skjermingsverdig eller annen sensitiv informasjon eller objekter kompromitteres. Ufullstendige risikobilder på virksomhetsnivå kan også gjøre det vanskelig for myndighetene å holde oversikt over den nasjonale sikkerhetstilstanden.

Økende kompleksitet og uoversiktlige systemer trekkes ofte frem blant årsakene til at sårbarhetene øker. Kompleksitet innebærer at det blir vanskelig å se hvordan påvirkning ett sted i systemet vil gi utslag andre steder. Vi kan ikke motvirke at digitale og samfunnskritiske systemer øker i mengde og blir mer sammenkoblet gjennom avhengigheter, men vi kan forsøke å redusere kompleksiteten ved å ha god oversikt over samfunnsviktige systemer og deres sårbarheter og risiko.

Sikkerhetsstyring i det daglige

Sikkerhetsstyring er et nødvendig virkemiddel for virksomhetens arbeid med å kontinuerlig forbedre sikkerheten.

I løpet av de neste årene forventer vi at flere objekter, infrastrukturer og informasjonssystemer vil identifiseres som skjermingsverdige. Vi forventer at norske virksomheter vil ha større behov for personell med sikkerhets- og adgangsklarering. Langt flere tjenester vil være tilkoblet internett, og verdien av den hurtig økende informasjonsmengden vil stige kraftig. For å redusere sårbarheter i samfunnsviktige systemer og virksomheter må det settes inn sikkerhetstiltak. Sikkerhetsstyring er i denne sammenheng avgjørende for at riktig tiltak identifiseres og iverksettes i takt med utviklingen.

Sikkerhetstiltak virker sammen og bør være en integrert del av virksomhetens styringssystem for å sikre at de riktige tiltakene implementeres og har ønsket effekt. NSM har gjennom en årrekke pekt på at mangelfull sikkerhetsstyring er en av de viktigste årsakene til utilfredsstillende sikkerhetstilstand.

Vår erfaring er at en del virksomheter har sikkerhetsdokumentasjonen på plass, men at tiltakene ikke er operasjonalisert og omsatt i sikkerhetskompetanse hos virksomhetens personell eller hvordan oppgavene løses i det daglige. Slike svakheter i sikkerhetsstyringen kan medføre at det forebyggende sikkerhetsarbeidet blir fragmentert. Mangler i sikkerhetsstyringen kan både skyldes, og føre til, en svak sikkerhetskultur i virksomheten. Godt forebyggende sikkerhetsarbeid krever at hele virksomheten er involvert, og at det er kultur for å melde fra når hendelser og avvik oppdages.

I møte med et stadig mer komplekst

Personellsikkerhetsmessige sårbarheter som ikke håndteres, kan fungere som inngangsporter for fremmede etterretningstjenesters arbeid med å rekruttere personell.

informasjonsdomene og et næringsliv preget av internasjonalisering, der sårbarheter forplanter seg raskt og virksomhetene knyttes sammen gjennom nettverk og avhengigheter, fører mangelfull sikkerhetsstyring og -ledelse til at de viktigste risikoene i virksomheter som forvalter sentrale norske verdier, ikke blir identifisert og redusert. Svært mange sårbarheter som holder døren åpen for en trusselaktør kan ledes tilbake til et sikkerhetsstyringssystem som kunne identifisert sårbarheten og sørget for at den ble lukket.

Personellsikkerhet som barriere

Innsiderrisikoen øker som konsekvens av at et større antall personer får tilgang til virksomheters verdier, og som et resultat av et trussel- og samfunnsbilde i endring. For at personellsikkerhet skal være en effektiv barriere som motvirker innsidervirksomhet og styrker sikkerhetsarbeidet, må virksomhetene ha et bevisst forhold til hvordan skjermingsverdig informasjon og andre verdier kan beskyttes gjennom bruk av autorisasjonsskiller og daglig sikkerhetsmessig oppfølging av personellet. Virksomhetene må også ha gode rutiner for å vurdere hvilke roller og tilganger som krever klarering og autorisasjon. Personell må bevisstgjøres, kompetanse må bygges og hendelser må håndteres for at personellsikkerhet skal ha ønsket effekt. NSM har sett eksempler på at personellsikkerhet vies for lite oppmerksomhet og at kompetansen på feltet er lav. Dersom personellsikkerheten ikke prioriteres, vil en innsider ha mulighet til å utføre stor skade mot en virksomhets verdier.

Svakheter eller mangler i virksomhetens personellsikkerhetsarbeid kan undergrave andre sikkerhetsbarrierer. Personellsikkerhetsmessige sårbarheter som ikke håndteres, kan fungere som inngangsporter for fremmede etterretningstjenesters arbeid med å rekruttere personell. Det vil også øke risiko for selvmotiverte innsidere. Konsekvensene av å nedprioritere personellsikkerhet er at virksomheter blir sårbare for både ubevisst og bevisst innsidervirksomhet, risikoen for sikkerhetsbrudd øker betraktelig og evnen til å oppdage innsidervirksomhet reduseres.

Sikring av samfunnsviktig informasjon og informasjonssystemer

Alle sikkerhetsregimer, enten gjennom sikkerhetsloven eller utenfor, eksisterer for å beskytte noe som er verdifullt for oss. Dette kan være selve funksjonene som understøtter våre grunnleggende nasjonale funksjoner, informasjonen om disse eller annen verdifull informasjon,

Helhetlig sikring av et objekt eller en infrastruktur innebærer å kjenne til avhengighetene til andre funksjoner og virksomheter, slik at også sikkerhetsnivået der blir tatt høyde for.

for eksempel planer og strategier. Informasjonssikkerhet går ut på å ha kontroll over konfidensialiteten, integriteten og tilgjengeligheten til informasjon man selv forvalter.

Samtidig er det en trend at virksomheter tjenesteutsetter driften av IKT-systemene sine eller flytter informasjonen til skytjenester. I de tilfellene der dette også betyr at informasjon forlater landet, er det flere momenter man må være klar over: For det første kan man miste kontroll over hvor informasjonen befinner seg både fysisk og juridisk, og for det andre vil man miste oversikt over hvem som har tilgang til informasjonen.

Antall informasjonssystemer øker. Informasjon blir digitalisert og dermed lettere tilgjengelig. Funksjoner som i dag ikke er heldigitaliserte, eller tilgjengelige via en digital inngangsport, vil i stor grad bli det i fremtiden. I digitaliserte virksomheter, der manuelle prosesser er i ferd med å fases ut, er IKT kjernevirksomhet uansett bransje.

I takt med digitaliseringen øker den potensielle angrepsflaten. God nettverkssikkerhet forutsetter god oversikt over egne nettverk. Desto større og mer sammenkoblede IKT-systemene blir, jo viktigere blir god sikkerhetsarkitektur og god segregering av nettverk. Når stadig flere verdier forvaltes av informasjonssystemer, blir konsekvensen at risiko øker for at vi vil oppleve kompromitteringer eller tap i samfunnskritiske funksjoner og infrastruktur.

Skjermingsverdige objekter og infrastrukturer

Helhetlig sikring av et objekt eller en infrastruktur innebærer å kjenne til avhengighetene til andre funksjoner og virksomheter, slik at også sikkerhetsnivået der blir tatt høyde for. Mens skjermingsverdige objekter kan beskyttes med fysiske og digitale barrierer, vil motstandsdyktighet i skjermingsverdig infrastruktur også bygge på redundans, dvs. reservesystemer eller parallelle systemer. NSM har sett eksempler på at innførte tiltak ikke har forventet eller planlagt effekt, og at f.eks. fysiske og digitale tiltak ikke ses i sammenheng, slik at man ikke oppnår helhetlig sikring.

I tiden fremover vil trusselaktører ta i bruk ny teknologi for å oppnå sine etterretningsmål. For å rustes mot fremtidige trusler er det viktig at skjermingsverdige objekter, infrastrukturer og andre viktige bygg og installasjoner er beskyttet av tiltak som tar hensyn til hvilke sikkerhetstruende hendelser de mest sannsynlig vil utsettes for. For å oppnå dette må sikkerhetstiltakene være basert på en

Offentlige virksomheter, både sivile og militære, blir i økende grad avhengige av privat sektor, og næringslivet vil i enda større grad levere tjenester og utstyr til sektorer av betydning for Norge i fremtiden.

helhetlig risikovurdering. Mangelfull oversikt over risiko og avhengigheter kan bety at sikringstiltakene blir for lite fleksible til å stå imot ulike etterretnings- og sabotasjemetoder.

Fysisk og digital sikring vil i fremtiden i større grad være gjensidig avhengig av hverandre. NSMs inntrengingstestere har ved flere anledninger forsert fysiske barrierer i norske virksomheter uten å bli oppdaget, bl.a. ved å følge etter ansatte med legitim adgang (såkalt tailgating), for deretter å få fysisk tilgang til nettverkspunkter. De har også oppnådd fysisk tilgang til virksomheter ved å kompromittere adgangssystemer via internett.

Privat understøttelse av viktige samfunnsfunksjoner

Offentlige virksomheter, både sivile og militære, blir i økende grad avhengige av privat sektor, og næringslivet vil i enda større grad levere tjenester og utstyr til sektorer av betydning for Norge i fremtiden. En rekke private virksomheter forvalter eller understøtter grunnleggende nasjonale funksjoner og andre viktige samfunnsfunksjoner. Offentlig sektor benytter i utstrakt grad konsulenttjenester og midlertidige ansatte fra næringslivet til å løse konkrete problemstillinger og oppdrag.

Næringslivsaktører som har en rolle i totalforsvaret, samarbeider med offentlig sektor eller på annen måte understøtter grunnleggende nasjonale funksjoner eller andre viktige samfunnsfunksjoner, kan være attraktive for fremmede etterretningstjenester. Det er sentralt at man på både offentlig og privat side forstår hvilken risiko man bærer på samfunnets vegne, og at man i sikkerhetsarbeidet vurderer og dimensjonerer risikoreduserende tiltak med dette som bakteppe.

Offentlige virksomheter som benytter næringslivsaktører som leverandører til viktige samfunnsfunksjoner, må derfor sørge for at leverandøren er i stand til å gjøre gode verdivurderinger av informasjon og andre verdier de håndterer og produserer på samfunnets vegne. En kompleks verdikjede med sviktende sikkerhetsstyring øker den samlede risikoen viktige samfunnsfunksjoner utsettes for.


SAS

Nasjonale risiko-reduserende tiltak

For å møte det komplekse trussel- og risikobildet innfører norske myndigheter stadig nye risikoreduserende tiltak. I denne delen beskriver vi noen av de mest sentrale grepene som gjøres og er gjort den senere tiden for å styrke det nasjonale sikkerhetsarbeidet.

Ny sikkerhetslov moderniserer og styrker sikkerhetsarbeidet

Hvorfor har vi fått ny sikkerhetslov?
1. januar i år trådte ny lov om nasjonal sikkerhet i kraft og erstattet sikkerhetsloven fra 1998. Behovet for ny regulering av det nasjonale sikkerhetsarbeidet skyldes særlig den raske og omfattende digitaliseringen av nær sagt alle samfunnsfunksjoner de siste 20 årene.

I driften av staten Norge i dag er offentlige, private, sivile og militære virksomheter koblet sammen i digitale økosystemer med uoversiktlige verdikjeder og avhengigheter som også strekker seg utenfor våre landegrenser. Mange private virksomheter leverer i dag tjenester som vi ikke klarer oss uten, både i det daglige og ved en krise. Både Forsvaret og sivile statlige organer er avhengige av private leverandører for å ivareta nødvendige funksjoner og tjenester. Den nye sikkerhetsloven har derfor et utvidet virkeområde, som i større grad enn den forrige loven griper inn i samfunnssikkerhetsdomenet og er ment å omfatte funksjonene, systemene og infrastrukturen vi ikke klarer oss uten.

Med digitaliseringen har også trusselbildet endret seg kraftig, til en situasjon der digitale trusler mot våre viktigste funksjoner, systemer og infrastruktur i form av spionasje og potensiell sabotasje dominerer. Demokratiske prosesser som valg og offentlig debatt utfordres flere steder i verden av påvirkningskampanjer og undergravende virksomhet gjennom bl.a. sosiale medier. Trusselbildet mot Norge og internasjonalt øker i kompleksitet, og preges ifølge Etterretningstjenesten av at utenlandske statlige og ikke-statlige aktører bruker et bredt spekter av virkemidler som kan ramme mål i flere sektorer.

I møtet med slike utviklingstrekk er en ny og moderne sikkerhetslov et helt sentralt grep fra norske myndigheter for å kunne styre risikoen bedre.

Hva er grunnleggende nasjonale funksjoner (GNF)?
Dette er landets viktigste funksjoner – dvs. tjenester, produksjon og andre former for virksomhet som vi ikke klarer oss uten. Dersom en slik funksjon faller bort, vil det ha konsekvenser for myndighetenes evne til å ivareta våre overordnede nasjonale sikkerhetsinteresser, dvs. Norges suverenitet, territorielle integritet og demokratiske styreform. De nasjonale sikkerhetsinteressene er videre inndelt i underkategoriene

a) de øverste statsorganers virksomhet, sikkerhet eller handlefrihet
b) forsvars-, sikkerhets- og beredskapsmessige forhold
c) forholdet til andre stater

Med begrepet forsvarlig sikkerhetsnivå stilles det nå krav til hva som skal oppnås, men ikke hvordan.

d) landets økonomiske velferd og trygghet
e) befolkningens grunnleggende sikkerhet og overlevelse

Departementene identifiserer GNF-er innenfor sitt ansvarsområde som faller inn under disse kategoriene.

Hva betyr forsvarlig sikkerhetsnivå?
Der den forrige sikkerhetsloven med forskrifter hadde en rekke detaljerte krav til sikkerhetstiltak, innfører den nye loven en funksjonell tilnærming. Med begrepet *forsvarlig sikkerhetsnivå* stilles det nå krav til hva som skal oppnås, men ikke hvordan. Dette gir virksomhetene fleksibilitet til selv å velge tilstrekkelige sikkerhetstiltak utfra egen risikovurdering. Begrepet forsvarlig sikkerhetsnivå gjør dermed lovens krav dynamiske ved at tiltakene kan tilpasses endringer i teknologiutviklingen og trussel- og risikobildet. Forsvarlig sikkerhet skal måles ut fra samfunnets behov i lys av hvilken samfunnsfunksjon virksomheten understøtter, og ikke utelukkende ut fra virksomhetens eget perspektiv. Det er også viktig å påpeke at virksomheten er avhengig av god sikkerhetskompetanse for å kunne oppnå et forsvarlig sikkerhetsnivå.

Hvilke virksomheter omfattes?
Loven omfatter statlige, fylkeskommunale og kommunale organer. I tillegg vil hvert departement ha ansvar for å vurdere hvilke private virksomheter som er av avgjørende betydning for grunnleggende nasjonale funksjoner og dermed skal underlegges sikkerhetsloven. Departementene skal også føre oversikt over hvilke private virksomheter som er av vesentlig betydning for GNF-ene. Disse virksomhetene skal imidlertid ikke underlegges sikkerhetsloven, og får dermed ingen plikter etter loven.

Hva kreves av virksomhetene som omfattes av loven?
Virksomhetene må gjennomføre risikovurderinger for å kunne identifisere hvilke sikkerhetstiltak som til sammen vil utgjøre et forsvarlig sikkerhetsnivå. I en slik vurdering er det viktig at virksomheten tar hensyn til hvilken betydning de skjermingsverdige verdiene den forvalter, utgjør for den eller de grunnleggende nasjonale funksjonene den understøtter og dermed for samfunnets behov. Denne risikobaserte tilnærmingen er en grunnpilar i den nye sikkerhetsloven, og hver virksomhet har et viktig ansvar for å sørge for at den ikke utsetter seg selv og samfunnsfunksjonene den understøtter for høyere risiko enn det som kan aksepteres.

Hvordan vil ny sikkerhetslov heve sikkerheten?

- **Sterkere ansvarliggjøring av departementene**

Loven legger et stort ansvar på departementene for forebyggende sikkerhetsarbeid innenfor sitt myndighetsområde. Dette innebærer å identifisere og holde oversikt over grunnleggende nasjonale funksjoner, hvilke virksomheter som er viktige for å understøtte disse funksjonene og hvilke som er så viktige at de skal underlegges loven innenfor departementets myndighetsområde. Denne prosessen vil i seg selv tegne et oppdatert kart over våre viktigste nasjonale funksjoner og virksomheter og avhengighetene mellom dem, som vil gi departementene, NSM og andre myndigheter verdifull informasjon for å holde oversikt over den nasjonale sikkerhetstilstanden.

- **Bedre samhandling, mer informasjonsdeling og bedre oversikt over sikkerhetstilstanden**

Loven legger opp til bedre samhandling og mer informasjonsdeling mellom myndigheter og virksomheter som er underlagt loven, bl.a. ved at NSM skal legge til rette for at trusselvurderinger og annen relevant informasjon tilflyter virksomhetene. Det skal også etableres fora for informasjons- og erfaringsutveksling mellom myndigheter og virksomheter. Økt samhandling og mer informasjonsdeling vil bedre virksomhetenes evne til å gjennomføre gode risikovurderinger og iverksette riktige tiltak og vil bidra til å heve sikkerhetskompetansen.

Samtidig har myndighetene behov for mer innrapportering av hendelser, trusler og sårbarheter for å kunne tegne et mer helhetlig nasjonalt bilde over sikkerhetstilstanden. NSM er gitt mandat til å innhente relevant informasjon fra virksomhetene som er underlagt loven, og virksomhetene plikter i tillegg å varsle NSM dersom de rammes av sikkerhetstruende virksomhet eller det har skjedd alvorlige brudd på sikkerheten. Økt informasjonstilfang og rapportering vil gi bedre oversikt over sikkerhetstilstanden.

- **Flere informasjonssystemer, infrastruktur og virksomheter underlegges loven**

Utvidelsen av lovens virkeområde innebærer bl.a. at et informasjonssystem kan underlegges loven på bakgrunn av dets funksjon snarere enn av at systemet er bærer av skjermingsverdig informasjon. Loven omfatter også infrastruktur i tillegg til objekter, fordi mange viktige samfunnsfunksjoner er avhengige av både enkeltinstallasjoner (et viktig enkeltstående bygg eller anlegg) og fysiske og digitale infrastrukturer

NSM registrerer med glede at IKT-sikkerhet kommer høyere på dagsorden og gis mer oppmerksomhet både på myndighetsnivå, i sektorene og blant virksomheter.

(f.eks. et styringssystem som styrer samferdselsfunksjoner). Det vil i mange tilfeller være private virksomheter som eier og forvalter informasjonssystemer og infrastruktur som etter ny lov vil bli utpekt som skjermingsverdig, noe som kan bety at flere private virksomheter blir underlagt loven. Etter NSMs syn betyr dette at nasjonal sikkerhet styrkes, bl.a. fordi det stilles høyere krav til sikkerhet for disse virksomhetene og fordi underleggelse til sikkerhetsloven gir myndighetene bedre oversikt over risikoen for funksjonene som virksomhetene understøtter.

- **Nødbremsen – regjeringens vedtaksmyndighet og eierskapskontroll**

Den nye loven gir regjeringen mulighet til å trekke i nødbremsen for å stanse oppkjøp av virksomheter som er underlagt loven eller annen aktivitet som kan innebære en risiko for våre nasjonale sikkerhetsinteresser. Dette er viktige hjemler for norske myndigheter for bl.a. å redusere risikoen for at utenlandske aktører bruker investeringer og oppkjøp for å få tilgang til norsk sensitiv informasjon, infrastruktur, høyteknologi eller naturressurser.

Styrking av nasjonalt cyber-sikkerhetsarbeid

Risikobildet knyttet til cybersikkerhet er komplekst og i rask utvikling. Effektive mottiltak krever koordinerte tiltak fra mange aktører, både offentlige og private.

NSM registrerer med glede at IKT-sikkerhet kommer høyere på dagsorden og gis mer oppmerksomhet både på myndighetsnivå, i sektorene og blant virksomheter. Vi mottar flere henvendelser fra ledernivå i norske virksomheter, bl.a. knyttet til vurderinger rundt tjeneste-utsetting. I flere sektorer etableres det eller er det allerede etablert regelverk knyttet til IKT-sikkerhet. Vi registrerer også at responsmiljøer for å håndtere IKT-hendelser, nye sikkerhetsselskaper og konsulenttjenester innenfor sikkerhetsfaget bygges opp.

Nasjonal strategi for digital sikkerhet

I januar i år lanserte regjeringen sin nye nasjonale strategi for digital sikkerhet[2], som trekker frem en lang rekke tiltak[3] for å styrke nasjonalt digitalt sikkerhetsarbeid. Blant disse er en pakke som bl.a. omfatter styrking av det nasjonale varslingssystemet for digital infrastruktur (VDI), neste generasjons nasjonale deteksjonskapasitet og

[2] Departementene (2019): Nasjonal strategi for digital sikkerhet.

[3] Departementene (2019): Tiltaksoversikt til nasjonal strategi for digital sikkerhet.

videreutvikling av NSMs Allvis Nor-tjeneste, som kartlegger sårbarheter i norske virksomheters tjenester på internett. Tiltakene omfatter også Nasjonalt cyberkrimsenter (NC3) under Kripos og Nasjonalt cybersikkerhetssenter, som etableres som en del av NSM i 2019.

Nasjonalt cybersikkerhetssenter

Det er i dag mange aktører som tilbyr råd og veiledning innenfor cybersikkerhet. Selv om arbeidet er godt, ser NSM økt behov for koordinering mellom ulike aktører. For at alle tilgjengelige ressurser skal utnyttes og trekke i samme retning, er det et uttalt behov å samle kompetansen innenfor cybersikkerhet på tvers av sektorer og miljøer, både for det offentlige og for private aktører som bidrar inn i dette arbeidet. Derfor etablerer NSM Nasjonalt cybersikkerhetssenter.

Nasjonalt cybersikkerhetssenter vil ha hovedansvar for koordinering og håndtering av nasjonale, sektorovergripende IKT-hendelser. Senteret skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringslivet mot cyberangrep. Det vil være et nasjonalt kontaktpunkt for cybersikkerhet, og vil samarbeide tett med relevante IKT-miljøer, akademia, eiere av kritisk infrastruktur og privat næringsliv både i Norge og utlandet.

Etableringen av Nasjonal cybersikkerhetssenter vil være komplementær til etableringen av Nasjonalt cyberkrimsenter (NC3) hos Kripos. Sammen vil disse kapasitetene dekke en helhet og på en mer effektiv måte utnytte summen av Norges cybersikkerhetsressurser.

Nasjonalt cybersikkerhetssenter – sentrale leveranser

- Løpende utvikling og deling av tiltak og anbefalinger om IKT-sikkerhet for å samordne og styrke digitalt sikkerhetsarbeid
- Samle sektorvise responsmiljøer, eiere av kritisk infrastruktur i privat næringsliv og akademia under samme tak
- Gjennom fysisk samlokalisering og delings-plattformer legge til rette for felles situasjons-forståelse, raskere informasjonsdeling og mer effektiv hendelseshåndtering
- Sikre best mulig samarbeid og effektiv nasjonal hendelseshåndtering
- Videreutvikle og tilgjengeliggjøre nasjonale tekniske sikkerhetstjenester

Under NATO-øvelsen Trident Juncture høsten 2018 var det utstrakt samhandling og koordinering mellom relevante cyberaktører på tvers av sektorer og myndighetsnivå, og rammeverket for håndtering av IKT-hendelser ble brukt.

NSMs Grunnprinsipper for IKT-sikkerhet
NSM har laget grunnprinsipper for IKT-sikkerhet[4] som flere virksomheter nå følger. Dette er et sett med grunnleggende prinsipper og tiltak for å beskytte informasjonssystemer. For å styrke IKT-sikkerheten i virksomheten er det viktig at ledelsen sørger for at risikovurderinger og tiltak gjennomføres etter anerkjente prinsipper. Samtidig som god grunnsikring og risikovurderinger er essensielt for å beskytte digital infrastruktur, er det ofte et spørsmål om tid før en virksomhet rammes av en digital hendelse.

Rammeverk for håndtering av IKT-sikkerhetshendelser
I tråd med stortingsmeldingen om digital sikkerhet fra 2017[5] har NSM utviklet et rammeverk for håndtering av IKT-sikkerhetshendelser. Rammeverket fastsetter prinsipper og ansvarsfordeling for hvordan IKT-sikkerhetshendelser skal håndteres. Under NATO-øvelsen Trident Juncture høsten 2018 var det utstrakt samhandling og koordinering mellom relevante cyberaktører på tvers av sektorer og myndighetsnivå, og rammeverket ble benyttet i myndighetenes krisehåndtering. Rammeverket for håndtering av IKT-sikkerhetshendelser er også blitt brukt i andre øvelser, så vel som i det daglige.

Sikkerhetsfaglige anbefalinger ved tjenesteutsetting
Det er et behov for at IKT-miljøene som forvalter virksomheters systemer profesjonaliseres og tilpasses deres behov. IKT-arkitektur må utvikles slik at sikkerhetsarbeid i større grad lar seg automatisere. Dette vil sørge for at riktige tjenester leveres, samtidig som det letter arbeidet med å holde systemer moderne og oppdaterte. Sluttbrukere må i større grad tilbys løsninger som fjerner eller reduserer risiko for brukerfeil. I de tilfellene hvor virksomheter setter ut tjenester til andre, endres den digitale risikoen virksomheten utsettes for. NSM har utarbeidet *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting*[6] som gir virksomheten råd om hvilke vurderinger som bør gjøres før man setter ut driften av IT-tjenester til andre.

Næringslivet som medspiller i sikkerhetsarbeidet

Private virksomheter spiller en sentral rolle i samfunnsutviklingen ved å være eiere og forvaltere av kritisk infrastruktur og andre sentrale samfunnsverdier, og ved å levere varer og tjenester til viktige samfunnsfunksjoner og i totalforsvarssammenheng. Offentlig-privat samarbeid er derfor også avgjørende innenfor sikkerhetsarbeidet. Samarbeidet mellom Næringslivets

[4] https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

[5] Meld. St. nr. 38 (2016–2017) IKT-sikkerhet – et felles ansvar

[6] https://nsm.stat.no/globalassets/dokumenter/tema-hefter/tjenesteutsetting2018v1.1_web.pdf

Sikkerhetsråd (NSR) og myndighetene er et viktig partnerskap i denne sammenhengen. NSR utgjør et bindeledd mellom offentlige sikkerhetsmyndigheter og næringslivet, og bidrar til å heve kompetanse og bevissthet om sikkerhetsspørsmål i næringslivet.

Økt samhandling og offentlig-privat samarbeid er et viktig moment i regjeringens nye nasjonale strategi for digital sikkerhet, og den nye sikkerhetsloven legger opp til større samhandling og informasjonsutveksling.

NSM har tatt initiativ til en kvalitetsordning for hendelseshåndtering. Formålet med ordningen er at virksomheter som opplever en IKT-sikkerhetshendelse skal kunne velge en kvalifisert leverandør av hendelseshåndteringstjenester. Det vil si at NSM har vurdert at leverandøren tilfredsstiller de kvalitetskrav som NSM har definert.

Innenfor kryptologifaget har NSM et tett og godt samarbeid med private aktører i norsk kryptoindustri. Dette samarbeidet omfatter både forskning og utvikling.

Profesjonalisering av personellsikkerhetstjenesten

Sikkerhets- og adgangsklarering er et sentralt virkemiddel for å sikre at kun personer med nødvendig pålitelighet, lojalitet og dømmekraft gis mulighet til å behandle skjermingsverdig informasjon og få innpass i skjermingsverdige objekter og infrastruktur. Geopolitiske og samfunnsmessige endringer fører til at den personellsikkerhetsmessige trusselen mot norske verdier er i stadig utvikling. Norske virksomheters behov for kompetanse, teknologi og leveranser fra utlandet må avveies mot sikkerhetsmessige vurderinger av hvem som kan gis tilgang til norske verdier. Slike utviklingstrekk utfordrer også klareringsmyndighetenes kompetanse, bl.a. når det gjelder i hvilken grad en persons bakgrunn, nasjonalitet eller annen form for tilknytning skal påvirke avgjørelsen om sikkerhets- eller adgangsklarering.

I 2018 ble det gjennomført et stort løft i profesjonaliseringen av personellsikkerhetstjenesten, ved at Sivil klareringsmyndighet ble opprettet for å samle alle klareringssaker i sivil sektor hos én virksomhet. Det er nå én stor klareringsmyndighet i forsvarssektoren og én i sivil sektor. Dermed vil man oppnå en mer profesjonalisert prosess og redusert saksbehandlingstid. Profesjonaliseringen gjør at NSM i større grad kan spisse sin rådgivningsaktivitet og være en mer synlig fagmyndighet innenfor personellsikkerhetsfeltet. Samlingen av klareringsmyndigheter vil være kompetansehevende ved at det etableres et miljø som kun fokuserer

Norske virksomheters behov for kompetanse, teknologi og leveranser fra utlandet må avveies mot sikkerhetsmessige vurderinger av hvem som kan gis tilgang til norske verdier.

på personellsikkerhet. Dette vil styrke de sikkerhetsfaglige vurderingene som gjøres, samt bidra til likebehandling og ivaretakelse av rettsikkerheten til personene som skal klareres.

Styrking av nasjonal sikkerhetskompetanse

Den raske teknologiutviklingen kan gjøre det utfordrende å henge med i sikkerhetsarbeidet. Krav om tilpassing til ny teknologi må balanseres med sikring av nettverk og datasystemer. Riktig kompetanse er avgjørende for å sikre informasjon, IKT-systemer og -infrastruktur. Kunnskap om sårbarheter og relevante sikringstiltak er viktig på alle områder som berører mennesker, organisasjoner og teknologi.

NSM erfarer at kunnskapsnivået i norske virksomheter ikke er tilfredsstillende når det gjelder sikkerhetsfaglig kompetanse og operasjonalisering av forebyggende sikkerhet. Mange sårbarheter ville trolig vært håndtert på en mer hensiktsmessig måte dersom virksomhetene hadde hatt bedre kompetanse. Riktig kompetanse kan heve kvaliteten på sikkerhetsarbeidet og bidra til bedre treffsikkerhet på hvilke sikringstiltak som implementeres. For å bidra til styrking av den nasjonale sikkerhetskompetansen videreutvikler NSM kurssenteret sitt og styrker rådgivningskapasiteten.

For å kunne beskytte verdiene våre nå og i fremtiden trenger vi forskning og utvikling både i forsvarssektoren, sivil sektor og i akademia. NSM har tidligere påpekt behov for generell sikkerhetskompetanse så vel som spesialistkompetanse innenfor IKT-sikkerhet.[7] Masterprogrammet i informasjonssikkerhet ved NTNU på Gjøvik er et viktig bidrag for å heve kompetansenivået, men det trengs flere studieplasser og kompetanseheving også innenfor andre sikkerhetsområder. Det er derfor positivt at regjeringen vil etablere et masterprogram innenfor sikkerhet og beredskap, hvor deltakere fra Forsvaret, Politiet, DSB, NSM, departementene og andre relevante aktører utdannes til samarbeid mellom sektorene og en felles forståelse av sikkerhets- og beredskapsarbeid.[8] Det er også forventet at satsningene i *Nasjonal strategi for sikkerhetskompetanse*, som blant annet omfatter styrking av digital sikkerhetskompetanse og styrking av nasjonal forskningskompetanse innenfor kryptologi, vil ha en positiv effekt.

I henhold til ny sikkerhetslov skal NSM legge til rette for at virksomheter som loven gjelder for, får tilgang til

[7] Bl.a. Risiko 2016, Risiko 2017 og Risiko 2018.

[8] Granavolden-plattformen, 15 – Forsvar. https://www.regjeringen.no/no/dokumenter/politisk-plattform/id2626036/#forsvar

Ny sikkerhetslov og nye forskrifter overlater mer av ansvaret for hva som er forsvarlig sikkerhetsnivå til virksomheten som eier og forvalter skjermingsverdig informasjon, infrastruktur eller objekter.

informasjon om trusselvurderinger og andre opplysninger som er av betydning for virksomhetenes sikkerhetsarbeid. Sammen med etablering av fora for informasjons- og erfaringsutveksling vil det bidra til utvikling og styrking av sikkerhetskompetansen i virksomhetene.

Ny sikkerhetslov og nye forskrifter overlater mer av ansvaret for hva som er forsvarlig sikkerhetsnivå til virksomheten som eier og forvalter skjermingsverdig informasjon, infrastruktur eller objekter.

For å hjelpe virksomhetene i dette arbeidet utarbeider NSM en rekke veiledere, blant annet i risikovurdering, skadevurdering av objekt og infrastruktur samt identifisering av grunnleggende nasjonale funksjoner. For å bidra til kompetanseheving og felles forståelse av ny lov og forskrifter, tilbyr NSMs kurssenter kurs innenfor flere av fagområdene knyttet til sikkerhetsloven. Kunnskap om det nye lovverket er sentralt for å lykkes i det forebyggende sikkerhetsarbeidet.

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

Tlf. 67 86 40 00
post@nsm.stat.no
www.nsm.stat.no