Rapport om sikkerhetstilstanden 2012

NSM

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) er det sentrale direktorat for beskyttelse av informasjon og infrastruktur av betydning for samfunnskritiske og andre viktige samfunnsfunksjoner. NSM skal innen sitt ansvarsområde skjerme informasjon og objekter gjennom å:

- Føre tilsyn og utøve myndighet i henhold til regelverk
- Varsle og håndtere alvorlige dataangrep
- Utvikle sikkerhetstiltak
- Gi råd og veiledning

NSM skal være en pådriver for bedring av sikkerhetstilstanden og gi råd om utviklingen av sikkerhetsarbeid i samfunnet.

Direktoratet er administrativt underlagt Forsvarsdepartementet og rapporterer til Justis- og beredskapsdepartementet for saker i sivil sektor.

Sammendrag

Norge og norske interesser utsettes daglig for uønsket og ulovlig etterretning. Det er en økning av avanserte spionasjeoperasjoner mot spesifikke mål av høy økonomisk eller samfunnsmessig verdi. Finanskriminalitet fra ikke-statlige aktører er av vedvarende høyt omfang. Det registreres flere og mer avanserte former for IKT-kriminalitet. Nettaktivisme og digitalt hærverk er gjengående fenomener som vil fortsette.

Sikkerhetstilstanden for 2012 er ikke tilfredsstillende. De sikkerhetsmessige utfordringene som er skissert vil fortsette, og øke i omfang. Dette begrunnes med markante sårbarheter på teknologiske, organisatoriske og menneskelige forhold. Det er registrert økt uønsket aktivitet mot viktige norske verdier. Sikkerhetsarbeidet i virksomhetene utvikles ikke tilstrekkelig for å møte et stadig mer komplekst risikobilde.

Virksomhetene, deres ledere og medarbeidere mangler ofte risikoforståelse og -erkjennelse. Dette er en grunnleggende årsak til svak håndtering av sikkerhetsutfordringer og sårbarheter. Det er også betydelige sårbarheter i informasjonssystemer, og mange virksomheter har ikke avholdt øvelser innen forebyggende sikkerhet. Det er urovekkende at innmelding av potensielt skjermingsverdige objekter ikke har funnet sted innen alle sektorer.

Visse sektorer er mer utsatt enn andre. Dette gjelder blant annet forsvarssektoren, forsvarsindustrien, olje- og gassektoren, luft- og romfartsindustri og annen høyteknologisk industri. I tillegg er beslutningstagere på sikkerhetspolitisk og utenrikspolitisk nivå utsatt.

Sikkerhet må følge teknologiutviklingen, og inngå i en helthetlig sikkerhetsstyring som også ivaretar stadig økende krav til effektivitet og samhandling. Det er et «våpenkappløp» mellom de som jobber med forebyggende arbeid gjennom beskyttelse og deteksjon, og de som utnytter sårbarheter for digitale angrep. Så snart det kommer et sikkerhetstiltak for å hindre utnyttelse, vil noen finne andre angrepsmetoder. Følgende sikkerhetsutfordringer må følges nøye fremover:

- Spionasje og kriminalitet gjennom bruk av IKT
- Nettbankkriminalitet, informasjonstyveri og hærverk på nett
- Sikkerhetsoppdateringer på systemer
- Store datamengder og nye lagringsløsninger
- Økt bruk av private enheter i arbeidssammenheng
- Industrisikkerhet
- Psykisk helse, økonomiske forhold og tilknytning til fremmede stater i forbindelse med sikkerhetsklareringer

Innledning

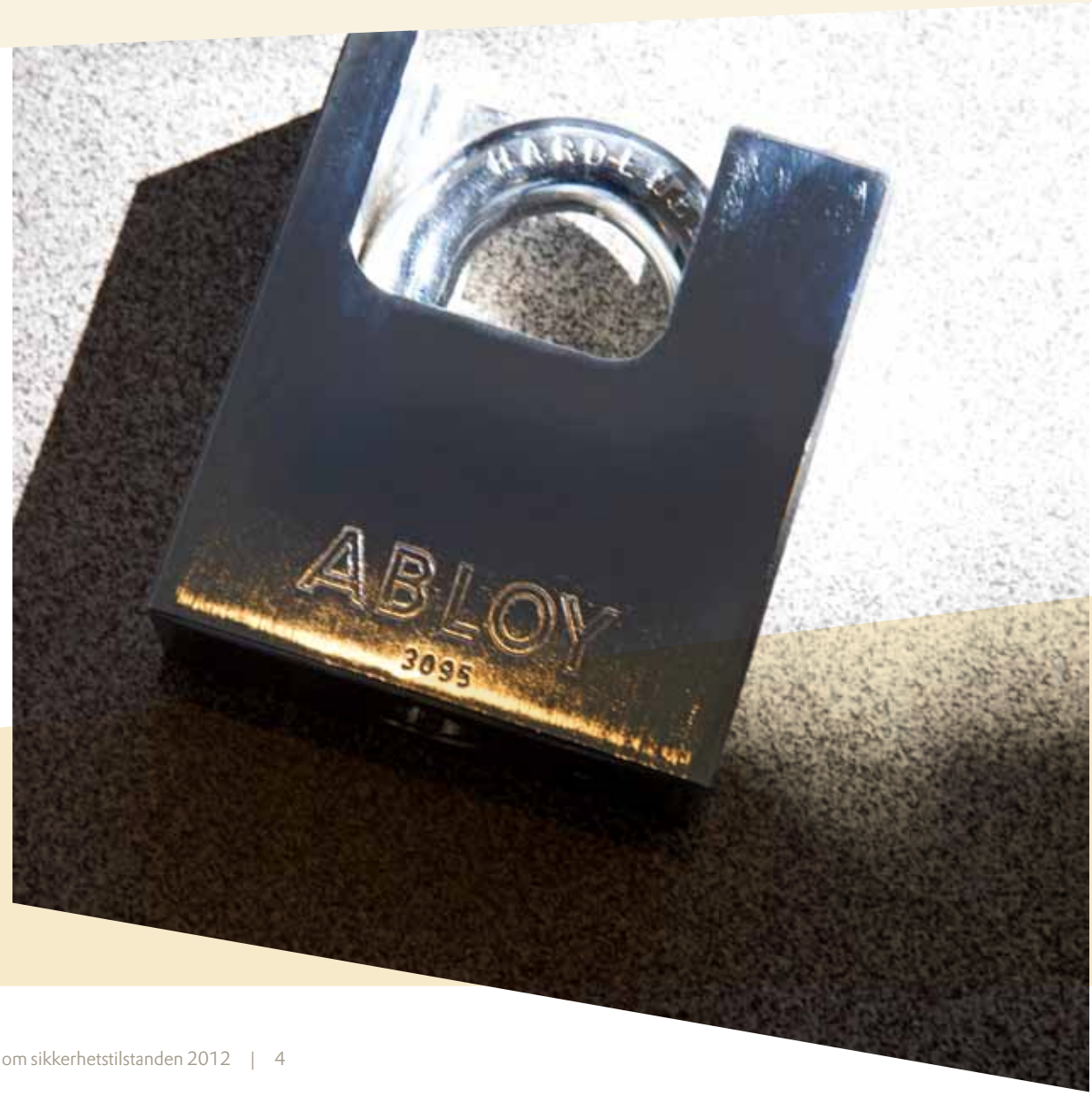
Norge har mange vitale verdier og interesser som må beskyttes mot trusselaktører.

Disse verdiene har ofte sårbarheter som trusselaktører kan søke å utnytte gjennom tilsiktede uønskede handlinger, blant annet i form av terrorisme, sabotasje, etterretning og andre kriminelle handlinger. Manglende evne til å vurdere risiko blir da bekymringsfullt. Sikkerhetstiltak vil mangle, feildimensjoneres, komme for sent, eller beskytte andre funksjoner og verdier enn tiltenkt.

Rapport om sikkerhetstilstanden gir en vurdering av sikkerhetstilstanden i Norge. Årets rapport påpeker sårbarheter som særlig kan eksponere norske interesser og samfunnsverdier for uønskede hendelser.

Rapporten er koordinert med Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten (E-tjenesten) med hensyn til trusselbildet.

Forebyggende sikkerhet skal bidra til å sikre nasjonale verdier i form av skjermingsverdige objekter og informasjon. Kompromittering, tap eller ødeleggelse av disse verdiene kan potensielt få store konsekvenser i form av blant annet tap av liv og helse, økonomiske tap eller begrensinger i suverenitet, styringsevne eller tillit til offentlige myndigheter. God sikring handler om å kjenne egne verdier, trusselen mot disse og sårbarheter som kan utnyttes, samt erkjenne samlet risiko. Dette bør følges opp med å vurdere og gjennomføre relevante og balanserte risikoreduserende tiltak.



Risikobildet

Norges interesser ivaretas gjennom trygg og god daglig forvaltning av sikkerhet og gjennom norsk sikkerhetspolitikk. Det er innenfor denne konteksten man må forstå nødvendigheten av forebyggende sikkerhet for å sikre Norges mest kritiske verdier.

Regjeringen har gjennom Soria Moria I- og Soria Moria II-erklæringene pekt på områder der Norge har særskilte interesser. Det pekes også på nye sikkerhetsutfordringer, blant annet terroranslag, og et behov for å styrke samfunnssikkerheten. Som en følge av Norges aktive deltagelse på den internasjonale arena stilles det nye krav til forebygging og sikring av gradert informasjon og skjermingsverdige objekter.

Risiko er uttrykk for forholdet mellom trusselen mot en verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen[1]. Risiko i tilknytning til samfunnssikkerhet er i stadig endring. Enkelte trusler endrer seg lite fra år til år, mens andre endres raskt og nye kan komme til.

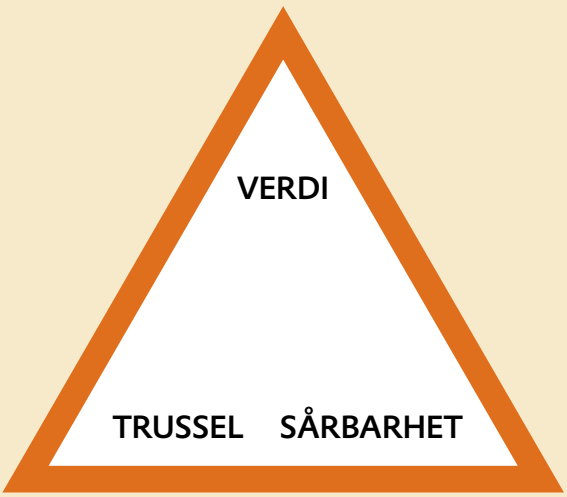
Formålet med risikostyring er å kontrollere og om mulig redusere risiko. Risikovurdering bidrar til dette og består av verdivurdering, trusselvurdering og sårbarhetsvurdering. Risikoen kan aksepteres som den er,den kan reduseres gjennom sårbarhetsreduserende tiltak, slik at nasjonale verdier og interesser sikres på en tilfredsstillende måte, eller den kan påvirkes ved å redusere eller eliminere trusselen.

1: Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Terminologi. Norsk Standard, NS 5830:2012

Hvordan vurdere risiko?

«Risikotrekanten» er et uttrykk for forholdet mellom en verdi, trusselen mot denne verdien, og sårbarheter som er knyttet til denne.

Kilde: Norsk Standard 5830:2012. Risikotrekanten benyttes i dag som rammeverk for NSM i vurderinger knyttet til risikobildet.



Nasjonale interesser og samfunnsverdier

Globalisering og annen samfunnsutvikling bidrar til et mer komplekst trusselbilde. Det kan være utfordrende å finne et akseptabelt risikonivå.

NSMs tilsyn og registrerte hendelser viser at det finnes manglende evne til å gjennomføre verdivurdering. Sikkerhetstiltak vil i så fall kunne mangle, feildimensjoneres, komme for sent, eller beskytte andre funksjoner og verdier enn tiltenkt. Verdivurdering er første trinn i en risikovurdering. Risikovurdering må inngå i virksomhetens kvalitetssikringsrutiner, slik at den blir en naturlig del av virksomhetens beslutningsprosesser.
De mest kritiske verdiene på nasjonalt nivå omfatter politisk krisehåndtering og forsvar av riket, befolkningens liv og helse, kritisk infrastruktur, økonomisk aktivitet av nasjonal betydning og nasjonens omdømme.

Noen samfunnskritiske virksomheter har verdier som er viktige for hele samfunnet. Dermed må de ivareta verdier som ikke bare gjelder egen virksomhet, men der bortfall av verdiene vil ha konsekvenser for hele samfunnet, direkte eller indirekte. For eksempel er de fleste sektorer avhengige av kraft og telekommunikasjon. Slike avhengighetsforhold kan krysse offentlige og private, sivile og militære, så vel som nasjonale og internasjonale skiller.

Andre eksempler på konkrete utsatte verdier er høyteknologi til petroleumsindustri, maritim industri, forsvarsteknologi, samt sensitive økonomiske og politiske vurderinger. Informasjon om krise- og beredskapsplanlegging innen disse områdene har potensielt høy verdi for trusselaktører. I tillegg er større menneskeansamlinger, som for eksempel idrettsarrangementer, konserter og trafikknutepunkt, verdier som kan være potensielle mål for terrorisme eller sabotasje.

I det daglige arbeidet i enkeltstående virksomheter er tanken om å beskytte Norges nasjonale verdier og interesser ofte ikke det mest nærliggende. Det kan likevel være avgjørende for en sektor eller et departement å vite hvordan enkeltstående virksomheter sikrer sine verdier på lokal- eller virksomhetsnivå. Dette er nødvendig for ikke å overse potensielt svake ledd i sikringskjeden.

Hva må beskyttes?

På nasjonalt nivå vil beskyttelse av informasjon og objekter[2] kunne være kritisk innen følgende områder:

Sikkerhetspolitisk krisehåndtering og forsvar av riket, herunder
- Beredskapsplaner; militære og sivile
- Informasjon om Forsvarets operative evne (materiell, infrastruktur, objekter, kapasiteter med mer)
- Kommando-, kontroll- og informasjonssystemer

Kritisk infrastruktur, særlig
- Kraft
- Telekommunikasjon
- Finans

Økonomisk aktivitet av nasjonal betydning, eksempelvis
- Olje- og gassindustri
- Maritim industri
- Finans- og bankvesen
- Forsvarsindustri

Beskyttelse av befolkningens liv og helse
- Bekjempelse av terrorisme og annen alvorlig kriminalitet
- Evne til å håndtere pandemisk sykdom.

2: Et skjermingsverdig objekt er eiendom, områder, bygninger, anlegg, transportmidler, annet materiell, eller deler av slik eiendom som kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser dersom de blir utsatt for terror- og sabotasjehandlinger.


HEMMELIG

Trusselbildet

Trussel defineres som *mulig uønsket handling som kan gi negativ konsekvens for sikkerheten til personer eller virksomheter.*[3] Trusselaktøren har intensjon (motivasjon) og kapasitet (evne) til å utføre en slik handling mot gitte verdier.

Det norske samfunnet utsettes for virksomhet som kan undergrave sikkerhet og skade nasjonale interesser. E-tjenesten og PST har blant annet fokus på trusselaktører og deres intensjon og kapasitet, samt hvordan disse kan true nasjonens sikkerhet og norske interesser i utlandet.[4] NSM legger blant annet disse vurderingene til grunn for rapport om sikkerhetstilstanden[5], samt kilder fra Kripos og ØKOKRIM. I tillegg er NSMs egne data, analyser og vurderinger om trusler i det digitale rom utgangspunkt for vurderingene.

Trusselaktører

PST og E-tjenesten vurderer fremmede staters etterretningstjenester som den største trusselen mot norske interesser. De er best organisert, har klar intensjon, høy kapasitet og vil kunne benytte flere metoder for å oppnå ønsket effekt. Fremmede staters etterretningstjenester er primært interessert i informasjon om: forsvars- og sikkerhetspolitikk, olje- og gassektoren, høyteknologi-, forskning- og undervisningsmiljøer og eksilmiljøer.[6]

PST vurderer at Norge og norske interesser daglig utsettes for uønsket og ulovlig etterretning fra andre stater. Dette innebærer løpende etterretning mot politiske prosesser, særlig knyttet til olje- og gass, Nordområdene og Svalbard. PST forventer et forsterket etterretningsfokus mot norske politiske prosesser innen disse områdene.[7] E-tjenesten vurderer at trusselaktører har evne til å manipulere andre staters beslutningsmekanismer og infrastruktur.[8]

Det digitale rom er en attraktiv arena for statsdrevne informasjonsoperasjoner. Denne type informasjonsoperasjoner utgjør den mest alvorlige formen for anslag mot kritiske IKT-systemer.[9] Flere nasjoner har bygget offensive kapasiteter for datanettverksoperasjoner. Disse vil kunne benytte et bredt spekter av metoder og virkemidler for å påvirke, og i verste fall sabotere, kritiske funksjoner og norske interesser i og utenfor territorielle grenser.

Eksempelvis påpeker E-tjenesten følgende i «Fokus 2013»: *Kinesiske myndigheter anvender i stor grad digitale operasjoner som en erstatning for menneskelig innsamling og bruker ofte stedfortredere for innhenting av informasjon. Lærersteder, bedrifter, organisasjoner og hackermiljøer gir et godt dekke for aktiviteten.*[10]

Finanskriminalitet fra ikke-statlige aktører er av vedvarende høyt omfang. Kriminell aktivitet på Internett antas å være av betydelig høyere omfang enn det som indikeres av antall saker som rapporteres eller politianmeldes. ØKOKRIM har vurdert skattekriminalitet, trygdebedragerier og korrupsjon som særlig alvorlig.[11] Risikoen for at virksomheter underlagt sikkerhetsloven blir utsatt for uønsket kriminell aktivitet via Internett eller mot graderte systemer vurderes å være økende. Forverringen i den internasjonale økonomien forventes å kunne føre til en økning i organisert kriminalitet. Nettaktivisme og digitalt hærverk er gjengående fenomener som vil fortsette.

Flere land fremmer sine interesser via frontselskaper, for å skjule statlig etterretningsaktiviteter. Dette skaper et uoversiktlig bilde over hvilke aktører som står bak informasjonstyveri.

Media har høsten 2012 omtalt en håndfull norske ekstreme jihadister som har tilegnet seg kamptrening i eksempelvis Syria. Konsekvensen av dette vil kunne være at norske interesser eller objekter (eksempelvis symbolbygninger) blir aktuelle mål. Det er en generell utvikling i dette miljøet at det tas i bruk virtuelle erfaringssentre, der det eksempelvis oppfordres til å angripe prosesskontrollsystemer og finansielle tjenester.

3: Jf NS 5830:2012.
4: For mer inngående vurderinger av trusselbildet, henvises det til E-tjenestens FOKUS 2013 og PSTs Åpen trusselvurdering 2013.
5: Rapport om sikkerhetstilstanden er en retrospektiv rapport. Rapporten avgir status for kalenderåret 2012. De trusselvurderinger som legges til grunn for årets RST, er således PST og E-tjenestens trusselvurderinger for 2012 (utgitt primo 2012).
6: PSTs Åpen trusselvurdering 2012.
7: Ibid.
8: E-tjenestens åpne vurdering, Fokus 2012, s. 26.
9: Høringsforslag fra Forsvaret ifm forslag til strategi for cybersikkerhet, datert 2010-05-04.
10: E-tjenestens FOKUS 2013.
11: ØKOKRIMs trusselvurdering 2011-2012, s. 9. Merk at ØKOKRIM benytter en annen type vurderingsakse i forhold til risiko, der konsekvens og sannsynlig er vurderingskriteriene for risikonivå.

Metoder og virkemidler
Det finnes en økning i antall avanserte spionasjeoperasjoner mot spesifikke mål av høy økonomisk eller samfunnsmessig verdi. Operasjonene kjennetegnes av at angriper forsøker gjentatte ganger selv om et angrepsforsøk blir avverget. Angriperen får ofte også fotfeste på IKT-systemet slik at angrepet ikke forsvinner selv om et angrep blir avslørt, et såkalt avansert utholdende angrep.

Antallet tilfeller av etterretnings- og spionasjeoperasjoner mot norske myndigheter og bedrifter som avdekkes har økt i 2012, samtidig som omfanget og kompleksiteten knyttet til hendelsene øker. Høyst sannsynlig er det et stort antall som ikke er avdekket, og sannsynligvis står samme aktør bak flere angrep. Flere av sakene har store likheter i metode og teknologi. Målet kan være å skaffe seg tilgang til, manipulere eller fjerne informasjon. Mer eller mindre sofistikerte sabotasje- og påvirkningsangrep har blitt rettet mot datasystemer som styrer industriprosesser og kritisk infrastruktur. Informasjonsinnsamlingen er ofte helhetlig og søker å utnytte alle mulige kilder med menneskelige, organisatoriske og tekniske svakheter eller sårbarheter.

Menneskelige faktorer spiller ofte en rolle i angrepsforsøkene. Sosial manipulering benyttes for å påvirke mennesker til å gi fra seg sensitiv informasjon eller utføre handlinger som de normalt ikke ville ha gjort. Dette er vanlig i kombinasjon med inntrenging i informasjonssystemer. Sosial manipulering kan skje under direkte menneskelig kontakt eller ved elektronisk kommunikasjon, som via e-post, direktemeldinger (chat) eller ved bruk av sosiale medier (Facebook, Twitter og andre sosiale nettverk).

Sårbarheter i nettlesere eller nettleserkomponenter utnyttes i større grad. Utnyttelse av sårbarheter i Oracle Java er blant de mest utbredte angrepsmåtene for øyeblikket. Dette ble eksempelvis observert ved et angrepsforsøk mot en norsk menneskerettighetsorganisasjon i 2012. Trusselaktører benytter seg av et såkalt vannhullsangrep, for å kompromittere brukere. I stedet for å angripe et spionasjemål direkte, kompromitteres en nettside som angriperen vet blir besøkt av målet, og blir infisert med angrepskode. Dette kan være vanskelig å oppdage, da nettsiden blir regnet som «trygg». Brukerne kan dermed bli kompromittert selv om de er bevisste på ikke å åpne mistenkelige vedlegg.

Det er ikke uvanlig at kriminelle på Internett kompromitterer websider og serverer angrepskode til besøkende. I slike tilfeller synes det å ligge økonomiske motiver bak. Denne type angrep gjør det også vanskeligere å detektere, analysere og håndtere hendelser i etterkant. Ingen vedlegg lagres på e-postserveren, og nettsideinnholdet kan endres raskt av angriper.
I april varslet NSM NorCERT om stor spredning av såkalt løsepengevirus. Dette ble spredd via norske nettsteder som var kompromittert gjennom annonsesystemene.
Alt elektronisk utstyr avgir stråling, og er dermed utsatt for informasjonsinnhenting. Metoder og utstyr som brukes i forbindelse med avlyttings- og avlesingsoperasjoner er under stadig utvikling. Slike operasjoner er svært vanskelig å detektere, fordi det sjelden legges igjen spor ved tapping av et system.

Alt fra enkle mikrofoner og kameraer til avansert utstyr er kommersielt tilgjengelig. Den kanskje største sårbarheten finnes i mobil- og smarttelefoner, lesebrett, mobile plattformer og lagringsmedier av ulike slag. Mobiltelefoner inneholder mye informasjon som uvedkommende ønsker tilgang til. Mobilbruk kan overhøres og mobiltelefoner kan spores, avleses eller avlyttes. Spionprogramvare og virus kan lett installeres på mobiltelefoner. I tillegg krever myndighetene i flere land av mobiloperatørene at det er mulig å avlytte mobil- og telenettet.

Sårbarhetsbildet

Sårbarhet defineres som *manglende evne til å motstå en uønsket hendelse eller å opprette en ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning.*[12] Virksomheter som har eller er avhengig av en verdi, vil også ha hovedansvar for å håndtere eventuelle sårbarheter knyttet til verdien og dennes funksjoner.

Det finnes vedvarende sårbarheter knyttet til sikkerhetstilstanden i virksomheter som har graderte informasjons- og kommunikasjonssystemer. I hovedtrekk er disse sårbarhetene knyttet til manglende risikoforståelse. Sårbarhetene kan være betydelige i de enkelte virksomhetene, men det er også bekymringsfullt at de vil kunne representere sårbarheter for andre eller for overordnede myndigheter. Sektorovergripende sårbarheter som potensielt får konsekvenser for hele samfunnet, er et kjennetegn på et samfunn som blir mer komplekst og utvikler gjensidige avhengigheter.

De sikkerhetsmessige utfordringene er annerledes i dag enn for ti år siden. Den internasjonale utviklingen fører til mer samarbeid og teknologisk og industriell utvikling på tvers av landegrenser. Beskyttelsen av norske interesser må tilpasses denne utviklingen. Det er et «våpenkappløp» mellom de som jobber med forebyggende arbeid gjennom beskyttelse og deteksjon, og de som utnytter sårbarheter for digitale angrep. Så snart det kommer et sikkerhetstiltak for å hindre utnyttelse, vil noen finne andre angrepsmetoder.

I tillegg til generelle sårbarheter og sikkerhetsutfordringer, trekker NSM frem fire fokusområder hvor utviklingen innebærer særskilte utfordringer for det forebyggende sikkerhetsarbeidet. Disse inkluderer det digitale rom, industrisikkerhet, personellsikkerhet og regelverksutvikling.

Generelle sårbarheter og sikkerhetsutfordringer

Måling av virksomhetsledere på sikkerhet
Forebyggende sikkerhet synes ikke å være forankret hos ledelsen i mange virksomheter underlagt sikkerhetsloven.[13] Dette gjør seg gjeldende gjennom manglende dokumentasjon og manglende etablering av internkontrollsystemer, som må være på plass for å bidra til at virksomhetens sikkerhetstjeneste revideres og forbedres. Vi tror at dette er knyttet til mangel på interne måleparametere knyttet til forebyggende sikkerhet og at ledere ikke måles på sikkerhet.

Informasjonssystemer i virksomheter
Mange virksomheter som behandler skjermingsverdig informasjon mangler graderte systemer på relevant nivå. Dette medfører at virksomhetene ikke har mulighet til å opprette nye dokumenter basert på innkommet informasjon, eller videreformidle denne elektronisk. Faren for feil gradering, eksempelvis av praktiske årsaker, er høyere der hvor de tekniske løsningene ikke er lagt til rette for de reelle behovene i virksomheten.

Selv med godkjente informasjonssystemer må krav til kontinuerlig risikostyring, bruks- og driftsinstrukser, rutiner for konfigurasjonskontroll med videre etterleves for at sikkerheten skal være tilstrekkelig ivaretatt. Mangler på disse områdene forekommer og medfører at en sikker tilstand ikke opprettholdes.

Beredskapsplanlegging og øving i virksomheter
Det er en rekke virksomheter som ikke har avholdt øvelser innen forebyggende sikkerhet. De har ikke øvet beredskapsplanen, og de har ikke øvd på tilintetgjøring av dokumenter og krypto i nødsituasjoner.

12: Ibid. Norsk standard 5830:2012.
13: Se rapport om sikkerhetstilstand 2010 og 2011.

Objektsikkerhet
NSM begynte å føre tilsyn med objektsikkerhet ved alle sine revisjoner høsten 2012. Det legges vekt på prosess for utvelgelse av mulige skjermingsverdige objekter, samt på styringssystem og risikovurderinger. Et skjermingsverdig objekt er eiendom, område, bygning, anlegg, transportmiddel eller materiell som ansees som helt essensielle for samfunnsviktige interesser. Arbeidet vil bli intensivert i 2013. Til sammen har NSM undersøkt utvelgelse av skjermingsverdige objekter ved åtte virksomheter i privat og offentlig sektor. Departementene skulle ha meldt inn oversikt over skjermingsverdige objekter innenfor sine sektorer innen 1. januar 2013. Etterlevelse av fristen er likevel variabel. Det er urovekkende at innmelding ikke har funnet sted innen alle sektorer. Det er utfordringer både innen sektorer og på virksomhetsnivå. NSM følger opp dette med råd, veiledning og møtevirksomhet.

Tekniske sikkerhetsundersøkelser (TSU)
NSM utførte i 2012 tekniske sikkerhetsundersøkelser ved flere titalls virksomheter/objekter. Nærmere 200 rom over flere tusen kvadratmeter ble gjennomsøkt.

Flere avvik ble avdekket. Mangelfull lyddemping (akustisk lekkasje) utgjorde over halvparten av avvikene, mens ikke tilfredsstillende rutiner knyttet til adgangskontroll utgjorde halvparten av observasjonene.

Inntrengingstesting
Inntrengingstesting av informasjonssystemer gjennomføres av NSM etter anmodning og samtykke fra den enkelte virksomhet. Testene avdekker hvor lett det er å hacke seg inn i datasystemer. Økende etterspørsel etter inntrengingstesting gir en viss optimisme i forhold til forankring av sikkerhetsarbeid i virksomheters ledelse. NSM registrerer at det i deler av statsforvaltningen gjøres et strukturert og effektivt arbeid for å bedre informasjonssikkerheten i egne systemer.

Inntrengingstestingen har avdekket sårbarheter og svakheter som går igjen i mange systemer. Dette gjelder både graderte og ugraderte systemer i sivil og militær sektor. Det er utstrakt bruk av svake passord, samt at programvare ofte er utdatert og sårbar. Sikkerhet i dybden praktiseres kun i liten grad, og totalt sett gir dette systemer som er svært sårbare for både målrettede og ikke-målrettede angrep.

Mange organisasjoner fokuserer på angrep fra utsiden, men er dårlig rustet til å motstå en kompromittering av sine systemer fra innsiden. Dette kan skje både gjennom sosial manipulering og innsidere, og kan øke skadeomfanget betraktelig.

Innrapporterte sikkerhetstruende hendelser
For virksomheter underlagt sikkerhetsloven gjelder lovpålagt rapporteringsplikt av sikkerhetstruende hendelser til NSM. Antall rapporterte sikkerhetstruende hendelser til NSM i 2012 var 109. Til sammenligning ble det i hele 2010 rapportert 35, og i 2011 rapportert 77 hendelser. Innrapporteringen gjør det mulig for NSM å ha en oversikt over hendelser som faktisk skjer. Vi ser altså en positiv utvikling, både med tanke på flere innrapporteringer og at flere ulike virksomheter rapporterer. Det antas at denne økningen primært reflekterer økt innrapportering.

Mørketallene anses å være store. Underrapportering og mangel på politianmeldelse av slike forhold kan komme av flere ting. Enkeltstående hendelser synes kanskje ikke viktige nok for den enkelte virksomhet. Innrapportering av flest mulig hendelser er imidlertid nødvendig for at NSM skal etablere et mest mulig helhetlig risikobilde. Flere av de innrapporterte hendelsene det siste året kan karakteriseres som alvorlige. Både privat og offentlig sektor er representert i materialet.

Det digitale rom

***Et forsvar for vår tid*, Prop.73 S (2011-2012), fremhever angrep i "det digitale rom "som en av de raskest voksende truslene mot privatpersoner, næringsvirksomhet og offentlige institusjoner. Angrepene går fort, metoder og virkemidler endres raskt og trusselaktøren kan være vanskelig å identifisere. De siste ti årene har det vært en endring i angrepsmetoder og i hvilke sårbarheter som utnyttes i det digitale rom.**

Spionasje
De siste årene har NSM sett en kraftig og klar økning i håndterte hendelser. NSM ser en ganske jevn kvartalsvis økning i totalt antall håndterte hendelser, og så langt viser utviklingen ingen tydelige tegn på å avta. Spesielt bekymringsfullt er det kraftig økende antallet av målrettede spionasjeoperasjoner mot norsk industri og norske interesser.

Vurderinger fra NSM og empiri fra åpne kilder og samarbeidspartnere tyder på at forsvarssektoren, forsvarsindustri, olje- og gassektoren, luft- og romfartsindustri og annen høyteknologisk industri er spesielt utsatt. I tillegg er beslutningstagere på sikkerhetspolitisk og utenrikspolitisk nivå utsatt.

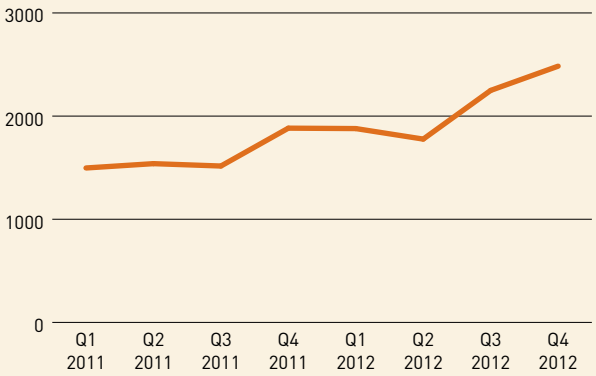
Etterretningstjenesten beskriver et bilde der avanserte statlige aktører står bak betydelig aktivitet i det digitale rom for å innhente sensitiv informasjon om andre lands disposisjoner, teknologi, økonomi og forsvar.[14] NSMs empiri understøtter dette. Det er økende aktivitet innen økonomisk, industriell, teknisk og annen ulovlig innsamling i det digitale rom.

Rammede virksomheters risikoforståelse er ofte mangelfull, og evnen til håndtering øker ikke proporsjonalt med antall hendelser.

Kriminalitet på nett
KRIPOS viser i sin trusselvurdering for 2012 til at IKT-kriminalitet antas å være langt mer utbredt enn det som fremgår av politiets statistikker. De siste årene er det registrert flere og mer avanserte former for nettbankbedragerier og hyppigere og mer alvorlige episoder av annen IKT-kriminalitet. I september 2012 var Norge på Europa-toppen. Årsakene er sammensatte, men samarbeid mellom aktører og grupper på tvers av landegrenser er blitt mer utbredt. Mange utenlandske grupper og nettverk har fått sterkere fotfeste i Norge.[15]

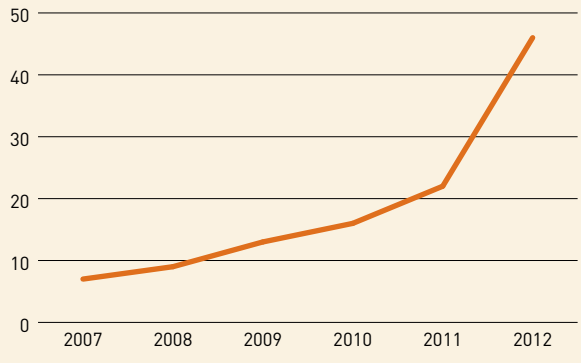
14: Etterretningstjenestenes ugraderte publikasjon Fokus 2012. Etterretningstjenestens vurdering.
15: Kripos: *Den organiserte kriminaliteten i Norge – Trender og utfordringer 2011 – 2012.*

HÅNDTERTE HENDELSER



Kvartalsvis utvikling i antall håndterte hendelser hos NSMs operative avdeling NorCERT, 2011 og 2012. Siste kvartal i 2012 ble det håndtert om lag 2500 hendelser. Til sammen ble det i løpet av året håndtert 8608 hendelser.

ALVORLIGE HENDELSER



Utviklingen i antall saker med høyeste prioritet, kategorisert som alvorlige, hos NorCERT fra 2007 til utgangen av 2012. I 2012 ble det totalt håndtert 46 alvorlige hendelser.

I 2012 har en rekke større norske nettsteder blitt kompromittert. Antallet har økt fra 125 i 2011 til 619 i 2012. Dette gjelder saker hvor websidene ikke bare er kompromittert, men hvor angripere forsøker å kompromittere besøkende på siden.

Angrep som skjer via kompromitterte nettsider er ofte vanskelig eller umulig å oppdage for de berørte brukerne. Man risikerer å bli kompromittert uten å gjøre noe aktivt på nettsiden ut over å besøke den, i motsetning til for eksempel angrep via e-post, hvor man gjerne må laste ned en fil eller åpne et vedlegg.

Tidligere har man gitt råd om å unngå «snuskete» sider på Internett for å redusere risikoen for å bli kompromittert, på samme måten som man gir råd om ikke å åpne e-postvedlegg fra ukjente. Siden 2007 har stadig flere legitime nettsider blir kompromittert, for deretter å spre skadevare til intetanende besøkende. Denne trenden har tiltatt de siste årene, og har i 2012 for alvor begynt å ramme norske nettsider. Det er en økende risiko for å bli kompromittert ved å besøke legitime norske nettsider. Et alvorlig aspekt ved dette er at personer og virksomheter i mindre grad kan redusere sin egen risiko for kompromittering ved å begrense sin ferdsel på Internett til det man anser som «trygge» nettsider.

Mange virksomheter bruker lang tid på å oppdatere sine systemer med siste sikkerhetsoppdatering. Selv om det finnes sikkerhetsoppdatering tilgjengelig, kan det på grunn av behov for testing i et komplekst driftsmiljø, ta måneder før virksomhetene har implementert alt. I mellomtiden vil de være sårbare.[16]

Det er de senere årene en økning i antall hendelser hvor aktivister har brukt Internett til å demonstrere, eller til å drive hærverk, skade eller på annen måte angripe personer, grupper eller virksomheter. Nivået på engasjement og kompetanse varierer over et bredt spekter blant aktivistene. Det finnes lavterskel aksjonsformer som tjenestenektangrep, hvor det krever lite kompetanse og liten innsats. Det finnes også mer avanserte angrep hvor aktivister digitalt bryter seg inn i informasjonssystemer og enten stjeler informasjon eller saboterer systemene. Det er observert tilfeller av alle formene i 2012.

Angrepsforsøk mot prosesskontrollsystemer (SCADA-systemer)

Stadig flere miljøer opparbeider seg kompetanse på innbrudd og påvirkning av overordnede elektroniske styringssystemer (SCADA[17]) i kritisk infrastruktur. Slike systemer er vanskelige å sikre. På grunn av den store sårbarheten i disse systemene er det stort behov for bedre kartlegging av trusler og sårbarheter, samtidig som kompetanse på området må utvikles.

Datalagre, skyproblematikk og big data

Skytjenester og lagring i «skyen» er blitt dagligtale de siste årene. Flere velger nettsky-løsninger for å håndtere sine datalagringsbehov. Store datasentre er i dag under utvikling og prosjektering. Mange offentlige og private samfunnskritiske tjenester har satt bort drift av servere og databaser til private datasentre, enten i form av egne datalagre eller skytjenester. Noen datalagre vil nødvendigvis komme til å lagre data av betydning for nasjonale interesser. Flere samfunnskritiske virksomheter kan ha lagret data i nettskyen. Dette er problematisk da det er vanskelig å ha kontroll på hvor data lagres, hvem som har tilgang, og hvor god sikringen er. God risikovurdering er nødvendig.

Big data blir omtalt som «den nye oljen», og kan generere betydelig økonomisk verdi i flere sektorer, blant annet gjennom økt produktivitet. Den teknologiske utviklingen gjør at det legges igjen svært mange digitale spor, ved surfing på Internett, bruk av telefon, bilkjøring, betaling med kort med mer. Andre nasjoner og store selskaper kan lagre og bearbeide svært mye informasjon om privatpersoner, virksomheter og staten. Dette kan skje uten at vi har oversikt over hvordan det skjer, og hva kunnskapen brukes til. I verste fall kan den brukes til å gjenskape informasjon vi ikke har hatt intensjon om å offentliggjøre, eller avdekke sårbarheter vi ikke selv er klar over.

16: NorCERTs kvartalsrapporter i 2012.
17: SCADA: Supervisory Control and Data Acquisition.

Bring Your Own Device (BYOD)[18]
Bruk av private digitale enheter på jobb, populært omtalt som Bring Your Own Device (BYOD), er en utvikling i store deler av arbeidslivet. Økende behov for mobilitet er en trend, særlig på lavgradert nivå. Hjemmekontor-ordninger etableres, og bærbare PC-er og nettbrett tas med på reiser både innenlands og utenlands. Dette medfører en rekke sikkerhetsmessige utfordringer, både for virksomhet og privatpersoner. Snart er mobilitet en problemstilling som gjelder flere tusen lavgraderte bærbare PC-er, og et enda større antall ugraderte men sensitive PC-er.

Man er på nett fra flere ulike enheter, for eksempel mobiltelefonen, hele tiden. Fra disse kobler man seg ofte opp til jobbens mailtjeneste, i tillegg til alle private tjenester. Denne sammenblanding av jobbenheter og private enheter gjør at sikkerhetsorganisasjonens evne til å gjennomføre risikoreduserende tiltak minsker.

Økt behov for integrerte systemer
Informasjonsutveksling innebærer sammenkobling av systemer. Det finnes sårbarheter knyttet til at brukere på et system kan få tilgang til data de ikke bør få tilgang til på et annet system. Konsekvensen av et innbrudd i et system kan også øke ved at tilgang til dette systemet igjen gir tilgang til andre systemer. Systemeierne må se mer helhetlig på det totale behovet for informasjonstjenester og planlegge de enkelte systemene ut i fra helheten. Flere tjenester flyttes fra dedikerte løsninger til ulike web-baserte tjenester. Det er en utvikling i retning av bruk av mer avanserte og interaktive web-tjenester eksponert mot Internett som stiller helt andre krav til sikkerhetsløsninger enn det man har hatt tidligere med mer statiske publikasjonstjenester. Løsningene blir ofte implementert uten at sikkerhetsmekanismene har blitt tilstrekkelig oppdatert for å møte det nye risikobildet.

Elektromagnetisk stråling fra IKT-systemer
Elektromagnetisk stråling handler om mulige utilsiktede sårbarheter som kan utnyttes til å få tilgang til sensitiv informasjon. Det er sårbarheter i alle typer IKT-utstyr, herunder kryptoutstyr, terminaler, tastatur, skrivere, skannere og kopimaskiner. Det finnes i dag ingen sivile standarder som fanger opp og vurderer slike sårbarheter i et IKT-system.

Å fly med sensor
All flygning med sensor over områder der man systematisk kartlegger[19], eksempelvis sjøbunn utenfor norskekysten[20], er underlagt nasjonale bestemmelser.

Denne type datafangst, når den er utenfor nasjonal kontroll, utgjør en sårbarhet, spesielt knyttet til sivil infrastruktur og ressurskartlegging. Store nasjonale og utenlandske aktører er meget pågående for å få NSM til å åpne for at denne typen datafangst kan gjøres av utenlandske leverandører.

18: "Ta med din egen dings", det vil sin inn i arbeidsgivers nettverk. BYOD er et begrep som beskriver at man bruker private mobile enheter i jobbsammenheng og kobler dem til arbeidsgivers systemer.
19: Kartlegging i denne sammenheng er systematisk innsamling av informasjon, herunder spesielt geodata.
20: Norsk territorium menes i denne sammenheng hele riket, herunder på Svalbard og Jan Mayen, samt på Bouvet-øya, og gjelder landområde, indre farvann og sjøterritoriet (under havoverflaten, samt over og under havbunnen), samt luftområdet over disse. Bestemmelsene knyttet til luftbårne sensorer gjelder ikke Dronning Maud Land og Peter I`s øy, jf. Forskrift av 2.5.1997 nr. 396 om adgang til opphold på norsk territorium under fredsforhold for fremmede militære og sivile statsfartøyer.

Personellsikkerhet

Personellsikkerhet dreier seg om tiltak, handlinger og vurderinger som gjøres for å hindre at personer som vil kunne utgjøre en sikkerhetsrisiko plasseres eller er plassert slik at risikoen aktualiseres. Det er spesielt en økning i tre typer saker som utfordrer kompetansen til klareringsmyndighetene, psykisk helse, økonomi og tilknytning til fremmede stater. Det som skaper størst kompetanseutfordring, er tilknytning til fremmede stater. Slike saker blir stadig mer ressurskrevende å vurdere.

Det finnes trusselaktører som søker å utnytte denne sårbarheten. De kan potensielt komme seg på innsiden av en virksomhet som besitter høygradert informasjon som kan misbrukes i terror og/eller sabotasjeøyemed eller til flyktningespionasje.

I Norge er det 45 klareringsmyndigheter, og sikkerhetsklarering gis på generelt grunnlag. Dette skaper utfordringer både når det gjelder rikets sikkerhet så vel som for enkeltindividets rettssikkerhet.

Industrisikkerhet

Norge har årlig et industrisamarbeid verdt 3 milliarder kroner i forsvarssektoren. Dette forplikter utenlandske leverandører for 9,5 milliarder kroner frem til 2018.[21] Norge er verdens andre største eksportør av gass, verdens sjette største eksportør av olje, har et av verdens største fond gjennom pensjonsfondet og er langt fremme på teknologi.

Norske virksomheter forvalter mengder av skjermingsverdig informasjon med skadepotensial. Kommer denne uvedkommende i hende, kan det påvirke Norges og alliertes forsvarsevne. Denne type informasjon vil kunne forenkle gjennomføring av spionasje, sabotasje og terror for en trusselaktør.

En rekke private virksomheter med ansvar for samfunnskritiske funksjoner er ennå ikke omfattet av sikkerhetsloven. Det betyr at mange potensielt skjermingsverdige objekter ikke har blitt identifisert og klassifisert og inntil videre faller utenfor det nødvendige sikkerhetsregimet, blant annet innenfor olje- og gassektoren, kraftsektoren og finanssektoren.

Sikkerhetsutfordringer ved Norges romvirksomhet

Norge har store ambisjoner i rompolitikken. Romprogrammet Galileo er utpekt som et flaggskip innen norsk romsatsning av både samfunnsnyttige og sikkerhetspolitiske hensyn. Galileo vil utfylle det allerede eksisterende GPS systemet.Gjennom Galileo-programmet utvikler EU et verdensomspennende sivilt satellittnavigasjonssystem (GNSS)[22].

Galileo vil få en økende verdi i samfunnet, som i større grad vil bli avhengig av systemet. Galileo vil de nærmeste år få økt strategisk og samfunnsøkonomisk betydning for Norge og vil med høy sannsynlighet utgjøre en viktig innsatsfaktor i samfunnskritisk infrastruktur og funksjoner. Dersom aktørene innen prosjektet ikke etterlever kravene innen forebyggende sikkerhet, vil en mulig konsekvens være svekket tiltro til nasjonens evne til å ivareta grunnleggende interesser for deltagerne og medlemslandene i prosjektet.

Anskaffende myndigheter og leverandører til store prosjekter

Stadig flere deler av utstyret i IKT-systemer inneholder komponenter fra et stort antall produsenter i mange land. Komponentene vil kunne være innom en rekke underleverandører, leverandører av delsystemer og logistikkorganisasjoner før endelig installasjon.

Komponentene produseres i hovedsak i land utenfor NATO. Det sammensatte produktet bør imidlertid være produsert i et alliert land (NATO-medlem eller lignende). Sikkerhet i leverandørkjeden mellom produsent og systemeier bør styrkes, eksempelvis i forbindelse med transport og mellomlagring. Dette er for øvrig en betydelig enklere problemstilling enn å sikre selve produksjonen.

Gjennom flere medieoppslag i 2012 ble det satt fokus på risikoen knyttet til bruk av elektroniske komponenter fra utenlandske selskaper i kritisk infrastruktur. Spesielt har kinesiskeide Huawei sin leveranse av Telenors nye 4G-nett vært nevnt.

Regelverksutvikling

For å kunne møte fremtidens utfordringer i det digitale rom, og forsterke og videreutvikle Norges evne til å håndtere IKT-baserte angrep mot samfunnskritisk infrastruktur og samfunnskritiske funksjoner, er det behov for et sterkere rettslig grunnlag.

Sikkerhetsloven slik den fremstår i dag er ikke dekkende for samfunnets sikkerhetsbehov. Det er en ambisjon å utvikle et sikkerhetsregelverk som tar utgangspunkt i hele samfunnets sikkerhetsbehov, uavhengig av organisatoriske tilhørigheter og skillet mellom gradert og ugradert informasjon.

21: Se www.regjeringen.no/nb/dep/fd/tema/anskaffelser_til_forsvaret/industrielt-samarbeid. Hentet 2012-12-01.

22: Systemet vil være interoperabelt med GPS-systemet. Galileo er Europas største industrielle fellesprosjekt. I Norge er det Nærings- og handelsdeparementet som tilrettelegger for norske bedrifter og deres adgang til og konkurransefortrinn i markedet. Under NHD er Norsk romsenter (NRS) nasjonalt prosjektkontor, og NSM har ansvar for GNSS systemets kritiske infrastruktur og samfunnsfunksjoner plassert på norsk territorium.

Veien fremover

Risikobildet er dynamisk, noe som må gjenspeiles i de sikkerhetstiltak som velges. Man må alltid leve med en viss grad av risiko. Utfordringen er å finne ut hva som er akseptabel risiko.

For å komme på et akseptabelt risikonivå er sårbarhetsreduserende tiltak nødvendig. I 2012 ble det igangsatt prosesser for å oppnå nettopp dette. Samtidig er det mye som fortsatt må gjøres for å møte både nåtidens og fremtidige sikkerhetsutfordringer. NSM skisserer nedenfor noen tiltak det anbefales å fokusere på i tiden fremover.

Anbefalte tiltak

Kompetanseheving på forebyggende sikkerhet
NSMs rapporter om sikkerhetstilstanden over flere år viser at kompetansen om forebyggende sikkerhet ikke er tilstrekkelig til at fagområdet får gjennomslag i virksomhetene. Det er nødvendig å etablere risikoforståelse og grunnleggende kunnskaper om sikkerhetsmessige utfordringer, samt måter å møte dem på. Det er særlig viktig å nå frem til ledernivå og påvirke ledelse til å sørge for adekvat sikkerhetsledelse i egen virksomhet. Det er også viktig å nå den enkelte medarbeider, da erfaring viser at den enkelte medarbeider er første linje med hensyn til å oppdage sikkerhetsmessig risiko. Det er også viktig å skolere dedikerte sikkerhetsmedarbeidere. Det må jobbes med sikkerhetskulturen i den enkelte virksomhet. Det må derfor utvikles fagplaner og undervisningstilbud tilpasset disse målgruppene. Kunnskap om sikring av IKT-systemer må forbedres.

Kompetanseheving kan gjennomføres med flere tiltak, som etablering av kurssenter, opplegg for e-læring og holdningskampanje både på nasjonalt nivå og i mindre skala.

Kompetansekrav for og organisering av klareringsmyndighetene
I dag er det ikke krav til kompetanse for å foreta sikkerhetsklareringer. Mange virksomheter kan sikkerhetsklarere. Det utgjør en utfordring med hensyn til forsvarlig og ensartet saksbehandling. Dette kan reguleres i forskrift. En form for sertifiseringsordning kan også vurderes.

Styrke den nasjonale evnen til å håndtere alvorlige IKT-hendelser
NorCERT gis en betydelig personellmessig styrking i 2013, og blir en del av Operativ avdeling i NSM sammen med blant annet kapasiteter for inntrengingstesting. Det er etablert gode rutiner for samarbeid med E-tjenesten, PST, Kripos og andre samarbeidspartnere i koordineringsgruppen for IKT-risikobildet. Disse rutinene er under videre utvikling.

Det anbefales å styrke nasjonal evne til å håndtere IKT-kriser ytterligere, blant annet ved å videreutvikle NorCERT som nasjonalt cybersenter.

På grunn av store sårbarheter for prosesskontrollsystemer (SCADA-systemer) i et stadig mer truende miljø, er det stort behov for økt kartlegging og kompetanse på området.

Revisjon av sikkerhetsloven
Sikkerhetsloven, og tilhørende forskrifter, har i 2011/2012 vært under en generell evaluering av en bredt sammensatt arbeidsgruppe ledet av Forsvarsdepartementet (FD). Arbeidsgruppens konklusjon er at lov- og forskriftsverk bør undergis en omfattende revidering med bakgrunnen den samfunnsmessige og teknologiske utvikling. FD, som regelverksforvalter av sikkerhetsloven, har gitt sin tilslutning til forslaget, og et revisjonsarbeid vil starte i 2013.

Øke innrapportering av sikkerhetstilstand og sikkerhetstruende hendelser
Regjeringen har besluttet at alle virksomheter i statsforvaltningen i løpet av 2013 skal vurdere sin sikkerhet og beredskap. Dette tiltaket vil bidra til en bevisstgjøring om sikkerhet. Resultatet vil bli fulgt opp av NSM. Det er ønskelig at dette tiltaket utvikles til en fast rutine. NSM vil også arbeide for bedret innrapportering av sikkerhetstruende hendelser.

Når NSM i fremtiden mottar sikkerhetsrapporter fra virksomheter i alle sektorer (via ansvarlige departementer), vil dette bedre evnen til å vurdere og analysere sektorvise og generelle sikkerhetsrelaterte situasjoner og trender, noe som igjen vil brukes som grunnlag for fremtidige tiltak for utbedring av sikkerhetstilstanden.

Nasjonal sikkerhetsmyndighet

Postadresse:
Postboks 14
NO-1306 Bærum Postterminal

Besøksadresse:
Rødskiferveien 20, Kolsås

Telefon: 67 86 40 00
Telefaks: 67 86 40 09

www.nsm.stat.no

Foto: Pål Rødah/Tinagent/NSM • Design: Markus Design AS