Nasjonal sikkerhetsmyndighet

NSMs Risikovurdering 2007

Gjennom Risikovurdering 2007 beskriver NSM viktige sider av risikobildet og redegjør for sikkerhetstilstanden. Basert på risikobildet og sikkerhetstilstanden gir NSM anbefalinger som har til formål å bedre det forebyggende sikkerhetsarbeidet på alle nivåer i samfunnet.

Forord

Samfunnet står overfor betydelige risikoer i form av spionasje, sabotasje og terror. NSMs risikovurdering for 2007 gir et bilde av hvordan vi som nasjon ved defensive tiltak kan forebygge slike trusler. I tillegg til å beskrive sikkerhetstilstanden gir vurderingen konkrete anbefalinger om hvordan vi kan forbedre oss.

NSMs risikovurdering viser hvor mangfoldig og mangeartet det forebyggende sikkerhetsarbeidet er. Det spenner fra arbeid med avansert teknologi til å vurdere personers lojalitet, pålitelighet og sunne dømmekraft. Mangfoldet kan også illustreres gjennom at NSM i 2006 har vært involvert i sikring av kritisk infrastruktur både i Antarktis og på Svalbard.

Vårt nasjonale sikkerhetsarbeid trenger flere løft. Ikke minst gjelder dette på IKT-siden. Nye investeringer er påkrevd for å erstatte gårsdagens løsninger. I årets vurdering foreslås ulike løsninger som gjør oss bedre i stand til effektivt å sikre skjermingsverdig informasjon.

Internett har gjort samfunnet mer effektivt. Informasjonsstrømmene går stadig raskere takket være Internett. Lanseringen av NorCERT er et viktig nasjonalt grep for å sikre kritiske infrastrukturer og samfunnsfunksjoner mot angrep over Internett. NorCERT er en viktig del av det nasjonale forsvar av et stadig mer digitalisert og nettverksorientert samfunn. Et slikt forsvar krever et tett samarbeid mellom offentlige og private aktører, hvilket NorCERT nettopp er.

Kjetil Storaas Hansen

Direktør

Sammendrag

NSM arbeider kontinuerlig med å vurdere hvilke virksomheter som bør omfattes av sikkerhetsloven. Et utgangspunkt her er virksomheter som inngår i kritisk infrastruktur og kritiske samfunnsfunksjoner. I så måte er olje- og gassektoren særlig relevant. Inkludering av samferdselssektoren er naturlig siden massetransportsystemer fremstår som mer sannsynlige terrormål. Andre områder av interesse er finanssektoren, IKT-sektoren, helsesektoren, kraftsektoren og satellittbasert infrastruktur.

Sikkerhetssamarbeidet med EU vil øke. Norsk deltagelse i *Battle Groups* og felles krisehåndteringsøvelser med EU er konkrete eksempler. En nærmere avklaring omkring sikkerhetssamarbeidet med EU er nødvendig.

Det blir stadig lagt ut sensitiv informasjon på Internett. NSM har i flere sammenhenger observert at det i kommentar og innleggssider med tilknytning til aktuelle saker legges inn informasjon om objekter som må antas å ha en sensitiv karakter. En ytterligere kilde til kompromittering er at skjermingsverdig informasjon i betydelig grad formidles via vanlig e-post.

Geografiske informasjonssystemer er et raskt voksende område innen IKT. Slike informasjonssystemer kan bli utsatt for målrettede IKT-angrep som kan svekke evnen til effektiv kriseledelse og krisehåndtering. Sårbarheten er særlig stor dersom slike systemer knyttes opp mot Internett. NSM har erfart at Internett og mobilnettet i stor grad benyttes som kommunikasjonskanaler under krisehåndtering. Både Internett og mobilnettet er sårbart. Det er viktig at andre IKT-løsninger må være på plass for å kunne sikre opprettholdelse av kommando og kontroll under en krisehåndtering.

NorCERT har registrert en sterk økning i bruk av botnett for å oppnå økonomisk vinning. Generelt utnytter organiserte kriminelle i økende grad teknologi for å oppnå økonomiske vinning. Bruk av phishing er et eksempel. Det er en sterk økning av antall ondsinnede koder som blir spredd gjennom Internett. Bruk av målrettede trojanere fremstår også som en sikkerhetsmessig utfordring. Generelt er det en utfordring å utvikle antivirusprogrammer og å gjennomføre nødvendige oppdateringer i de ulike nettverk.

NSM mener det er behov for en større nasjonal cyberøvelse i Norge. En cyberøvelse er viktig for å avdekke forbedringspunkter i vårt nasjonale krisehåndteringsapparat.

Innledning

Forebyggende sikkerhetstjeneste i henhold til sikkerhetsloven skal gi samfunnet en grunnsikring mot spionasje, sabotasje og terrorhandlinger. Alle offentlige og private virksomheter underlagt sikkerhetsloven skal ha på plass et tilstrekkelig utvalg av forebyggende sikkerhetstiltak. Summen av egensikringen i den enkelte virksomhet utgjør en viktig del av samfunnets samlede grunnsikring. Spørsmålet vi alltid må stille oss er om vi beskytter det som har størst verdi. Utfordringen er å kunne identifisere hvilken informasjon og hvilke objekter vi skal skjerme av hensyn til rikets selvstendighet og sikkerhet, samt andre vitale nasjonale sikkerhetsinteresser. En annen viktig del av risikobildet er å kunne identifisere egne svake punkter eller sårbarheter.

NSMs risikovurdering benytter ulike kilder, blant annet funn fra NSMs tilsyns- og besøksaktivitet og rapporter tilsendt NSM sikkerhetstruende hendelser. Gjennom deltagelse under øvelser har NSM skaffet seg innsikt i hvordan det forebyggende sikkerhetsarbeidet fungerer i forbindelse med krisehåndtering. Risikovurderingen drar også nytte av NSMs egen fagekspertise innen IKT, fysisk sikring, personellsikkerhet, sikkerhetsgraderte anskaffelser, sikkerhetsadministrasjon, dokumentsikkerhet og objektsikkerhet. NorCERT er en viktig leverandør av informasjon omkring faktisk aktivitet på Internett og omkring forventede sikkerhetsrelaterte utviklingstrekk og utfordringer på nettet. NSM innhenter også viktig trusselinformasjon fra Etterretningstjenesten (E-tjenesten) og Politiets sikkerhetstjeneste (PST). NSM er videre aktive i en rekke nasjonale råd og utvalg som bidrar til å gi innsikt i forhold med relevans for både risikobildet og sikkerhetstilstanden. Den brede internasjonale kontaktflaten er også en vesentlig kilde til informasjon. NSM benytter også arbeider fra forskningsinstitusjoner som grunnlagsmateriale i risikovurderingene.

Trusselbildet

Kjennskap til trusselaktørenes intensjoner, kapasiteter og metoder er viktig for hvordan egensikringen innrettes. PST fastsetter det nasjonale trusselnivået og utarbeider utfyllende trusselvurderinger. Etterretningstjenesten beskriver trusselnivået i områder utenlands hvor Norge har særlige interesser.

Viktigheten av god informasjonssikkerhet understrekes av at PST vurderer etterretningstrusselen mot Norge og norske interesser til å være betydelig. PST slår fast at flere stater utfører etterretningsvirksomhet mot norske interesser. Kompromittert informasjon

omkring militære planverk eller kapasiteter kan bidra til å svekke eller vanskeliggjøre eventuelle militære operasjoner hjemme og ute, samtidig som egne og alliertes liv kan settes i fare. PST mener etterretningsoffiserer forsøker å påvirke premissleverandører og enkeltpersoner i de politiske beslutningsprosessene. For norske bedrifter vil etterretningsvirksomhet kunne føre til svekket konkurranseevne, reduserte markedsandeler og tap av inntekter og arbeidsplasser. Det er grunn til å anta at norsk politikk og næringsaktivitet tilknyttet nordområdene er av interesse for utenlandsk etterretning. Kriminelle miljøer driver målrettet innhenting av informasjon. Kriminalitet kan også utgjøre en trussel for skjermingsverdig informasjon og skjermingsverdige objekter. I operasjonsmanualer tilhørende al-Qaida nettverket beskrives innhenting, systematisering og analyse av informasjon som en kjerneaktivitet.

Det fins flere muligheter til å innhente informasjon. NSM har i tidligere vurderinger listet ulike mulige plattformer for etterretningsinnhenting, herunder utenlandsk personell i Norge, skipsfart, IKT-systemer, Internett, elektroniske innsamlingssatellitter og fotosatellitter, teknisk avlyttings- og avtittingsutstyr, reiser og delegasjoner, observasjon, bruk av vervede personer og bruk av åpne kilder.

Trusler fra al-Qaida-nettverket mot Norge og norske interesser i mai 2003 og oktober 2004 bidro til at PST høynet det generelle trusselnivået til MODERAT. Det generelle trusselnivået ble tilbakeført til LAV i juni 2006. I september 2006 ble det tatt ut siktelse mot fire personer i forbindelse med skytingen mot synagogen i Oslo, videre i forbindelse med at det ble fattet mistanke om aksjoner mot amerikanske og israelske mål i Norge. Dette medførte ingen heving av det generelle trusselnivået. Britiske myndigheters avsløring av planer om å sprenge et større antall fly i august 2006, medførte heller ikke til en heving av det generelle trusselnivået. Derimot manifesterte det sistnevnte seg i strengere internasjonale sikkerhetstiltak for lufthavner.

Terrorister med et globalt nedslagsfelt har intensjon og kapasitet til å ramme vestlige interesser og verdier. Norge i egenskap av å være en del av Vesten står derfor overfor et endret risikobilde, som kan endres på kort tid eller uten varsel.

Den lave, men diffuse terrortrusselen er vanskelig å måle, den er lite presis og den kan derfor være vanskelig å forholde seg til. Erfaringsmessig fremstår massetransportsystemer som attraktive mål for terrorister. Med det som bakgrunn tok Øvelse Oslo 06 utgangspunkt i terroranslag mot tog, T-bane og buss. Øvelsen var den første større sivile terrorøvelsen i Norge. Bakgrunnsscenariet var hentet fra terrorhendelsene i Madrid mars 2004 og London juli 2005.

Sikkerhetslovens virkeområde

Flere private virksomheter bør inn under sikkerhetslovens virkeområde for å legge til rette for en bedre egensikring, og fordi informasjon og objekter som er skjermingsverdige i dag ligger utenfor lovens rekkevidde. I forbindelse med egensikringen vil det også være aktuelt for en rekke virksomheter å motta trussel- og risikoinformasjon fra myndighetsorganer som PST og NSM. Håndteringen av slik informasjon krever at sikkerhetsloven gjøres gjeldende for mottakerne.

Et viktig utgangspunkt her er virksomheter som inngår i kritisk infrastruktur og kritiske samfunnsfunksjoner. Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner, som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse. Olje- og gassektoren med produsenter og eiere av kritisk infrastruktur er særlig relevant. Inkludering av flere virksomheter innen samferdselssektoren vil være en naturlig respons på at massetransportsystemer fremstår som mer sannsynlige terrormål. Andre områder av interesse er finanssektoren, IKT-sektoren, helsesektoren, kraftsektoren og satellittbasert infrastruktur.

Standardene i sikkerhetsloven med forskrifter gir en helhetlig tilnærming til forebyggende sikring og er i hovedsak tilgjengelige for alle. Sikkerhetsklarering av personell er et av unntakene. Virksomheter som ikke faller inn under sikkerhetsloven, kan benytte alle de standarder de for øvrig måtte finne aktuelle for sin egensikring. På denne måten bidrar sikkerhetsloven med forskrifter og veiledninger til å styrke sikkerheten utover det avgrensede virkeområdet for loven.

Verdivurdering, hva er viktig å beskytte?

Hensikten med verdivurdering er å bidra til at riktig informasjon og riktige objekter skjermes. Til sammen bidrar systematiske verdivurderinger til å skape et robust samfunn, som er bedre beskyttet mot terrorhandlinger, sabotasje og etterretning. Alle virksomheter underlagt sikkerhetsloven skal bidra til å peke ut hvilken informasjon og objekter som må skjermes. NSM har sett en positiv trend med hensyn til fokus på verdivurdering i året som har gått. Flere virksomheter har erkjent hvorfor en systematisk verdivurdering er nødvendig.

Endringer i våre omgivelser, eksempelvis den overordnede sikkerhetspolitiske, teknologiske, samfunnsmessige og økonomiske påvirker løpende hva vi ønsker å skjerme. Endringer i myndighetenes prioriteringer kan også måtte legges til grunn under en verdivurdering. Regjerings fokus på FN og Nordområdene fremstår her som to konkrete eksempler. Dersom politiske områder med bæring på nasjonale sikkerhetsinteresser prioriteres, øker også sannsynligheten for at saksområdet inneholder kategorier av informasjon som bør verdivurderes opp mot sikkerhetsloven. Et annet forhold som må vektlegges under en verdivurdering, er Norges rolle som småstat. Som småstat er det i mange sammenhenger viktig å holde en kjerne av informasjon skjermet fra omverdenen. Videre er Norge som småstat særlig sårbar med tanke på evne til å oppnå egne målsettinger. Ettersom en småstats handlingsalternativer er begrensede, og maktmidlene få, er det viktig med en bevisst informasjonssikkerhet. For en småstat fremstår informasjon som en særlig kritisk ressurs.

Under en verdivurderingsprosess er det viktig å koordinere egen verdivurdering med andre aktuelle virksomheter. Dersom andre virksomheters verdivurdering anses som overdreven eller mangelfull må den andre virksomheten gjøres oppmerksom på det. NSM har sett flere eksempler på at virksomheter ikke koordinerer egen verdivurdering med andre relevante virksomheter.

I forhold til eksempelvis terrortrusselen kan folks årvåkenhet være avgjørende for å være i stand til å avdekke eventuelle planlagte anslag. Generelt er politiet avhengig av tips og informasjon fra befolkningen. For å sikre en god bevissthet i befolkningen er det således viktig å informere om hva man bør være på vakt overfor. I lys av dette er det viktig å finne en fornuftig balanse mellom hva som holdes skjermet og hva som kan bli offentliggjort.

NSM vil anbefale at den øverste ledelsen i virksomheter hvor sikkerhetsgradert informasjon blir håndtert, tar tilstrekkelig hensyn til verdivurdering. NSMs veiledning i verdivurdering er et hjelpemiddel for å imøtegå dette. Minst en person i en strategisk ledergruppe bør gis et særlig ansvar for å gi innspill omkring verdivurdering. Det kan vises til at funksjonen informasjonssikkerhet ofte inngår i den øverste ledelsen i en del større private virksomheter. Følgelig vil ledelsen bli mer involvert i egen virksomhets vurdering av egen informasjons eventuelle skjermingsverdighet.

Internett og informasjonssikkerhet

Internett blir brukt til etterretningsinnsamling. Internett fremstår som et medium hvor informasjon har et tilnærmet ubegrenset spredningspotensial. Legges sensitiv informasjon ut på Internett vil denne informasjonen være tilgjengelig for hvem som helst. Sensitiv informasjon på Internett gjør skadepotensialet ekstra stort fordi alle kan laste den ned. Samtidig er det tilnærmet umulig å etterspore spredningen av utlagt informasjon, potensialet for spredning er i prinsippet uendelig. Det er i praksis umulig å trekke tilbake informasjon som er publisert på Internett. Internett har den egenskapen at informasjon som publiseres for et lokalt publikum, har global tilgjengelighet. Dessuten blir informasjon som ikke er skjermingsverdig når trusselbildet er lavt, skjermingsverdig når trusselen øker.

Informasjon tilknyttet saksbehandling formidles ofte på e-post og bidrar til effektiv saksbehandling. Likevel er det viktig å erkjenne de ulike sikkerhetsrelaterte farekildene som tilligger bruk av Internett og e-post. I året som har gått er det kjent fra media at det i statsforvaltningen er feilsendt e-post med politisk sensitiv informasjon. Slike feilsendinger kan fort skje dersom e-post adresser ligner hverandre. I tillegg kan den oppgitte avsenderen av informasjon være falsk. Det finnes heller ingen garanti for at innkomne meldinger ikke blir manipulert.

Alle virksomheter bør utarbeide egne retningslinjer for bruk av Internett. I slike interne retningslinjer anbefales det fastsatt hvilken informasjon som ikke kan formidles på ubeskyttet e-post. Det er også en anbefaling at virksomhetens intern-kontrollrutiner inkluderer egen bruk av Internett.

I dag utvikler de ulike virksomhetene ofte egne graderte informasjonssystemløsninger. Denne utviklingen skjer ofte uten at allerede sikkerhetsgodkjente løsninger gjenbrukes. Ulike løsninger gjør det krevende å koble systemer sammen og kommunisere på tvers av virksomheter. NSM mener at større grad av gjenbruk av sikkerhetsgodkjente løsninger, innen både militær og sivil sektor, vil bidra til bedre sikkerhet.

Mange er avhengige av bærbare PC-er i jobbsammenheng. Av den grunn foreligger det et behov for å finne frem til sikkerhetsløsninger som er tilpasset vår PC-bruk. Ved tap av PC-en vil godkjent kryptering av harddisken gjøre det tilnærmet umulig for en aktør å tappe den for informasjon. Diskkrypteringen bør med ulik innkapsling kunne benyttes av både militære og ulike sivile virksomheter.

Nødnett-prosjektet er et betydelig løft for sentrale deler av samfunnssikkerheten og krisehåndtering på ulike nivå. For å forebygge at systemet misbrukes eller bevisst forstyrres er det viktig at systemet gjøres mest mulig robust.

Geografiske informasjonssystemer (GIS)

Bruken og utbredelsen av geografiske informasjonssystemer (GIS) øker. GIS bidrar til en effektiv tilrettelegging av informasjon til bruk i samfunnssikkerhets- og beredskapsarbeid. GIS-løsninger kan benyttes for å vurdere risikoforhold, etablere et situasjonsbilde, som støtteverktøy for varsling og evakuering, som støtteverktøy for etablering av beredskapsordninger og som støtte til planlegging og styring av operativ virksomhet.

Internasjonalt brukes GIS i økende grad i samfunnssikkerhets- og beredskapsarbeid. En EU-relatert GIS-bruker er *Monitoring and Information Centre* (MIC), som er en del av *The European Community Civil Protection Mechanism*. Senteret bruker GIS i forbindelse med situasjonsovervåkning, skadevurderinger og varsling. MIC tilbyr døgnbasert støtte ved alvorlige hendelser innen EU. I Norge benyttes stedfestet informasjon og geografiske informasjonssystemer i økende grad. Blant annet gjelder dette innenfor alarmberedskap og utrykning hos hovedredningssentralene, politiets operasjonssentraler, de fleste alarmsentraler for brann og ambulanse og i Forsvaret.

GIS koples i økende grad sammen med GPS. Sammenkoplingen gjør at det kan fremskaffes sanntids oversiktsbilder av hvor personell eller materiell befinner seg. Ved å sammenstille geografisk informasjon fra ulike datakilder fremskaffes et mer fullstendig oversiktsbilde. Et slikt oversiktsbilde kan samtidig kobles til personopplysninger, bedriftsinformasjon, informasjon om kritisk infrastruktur og kritiske samfunnsfunksjoner, informasjon om materiellmessige og personellmessige kapasiteter til bruk i krisesituasjoner. Informasjonssystemer med store mengder ajourført informasjon til bruk i samfunnssikkerhets- og beredskapsarbeidet på lokalt, regionalt eller nasjonalt plan, har en betydelig etterretningsmessig verdi. Slike informasjonssystemer kan også bli utsatt for målrettede IKT-angrep med formål å svekke evnen til effektiv kriseledelse og krisehåndtering, særlig dersom de knyttes opp til Internett.

Utfordringer tilknyttet krisehåndtering og øvelser

Det meste av forebyggende sikkerhetstjeneste i en normalsituasjon, er også en forberedelse til håndteringen av kriser og krig. Det er avgjørende at virksomhetene opererer med dette perspektivet. Alle offentlige og private virksomheter, som inngår i vårt nasjonale krisehåndteringsapparat, må ha fokus på informasjons- og objektsikkerhet. God krisehåndtering forutsetter forberedelser i en normalsituasjon. Ved en oppstått krisesituasjon er det avgjørende at organisatoriske, materielle, kompetansemessige og planmessige forhold er på plass. Etter en reell krisehåndtering, eller etter en øvelse, er det viktig at også den forebyggende sikkerheten evalueres. Basert på erfaringer kan det nasjonale krisehåndteringsapparat forbedres. Under øvelser trenes vårt handlingsmønster og planverk i tilfelle en krisesituasjon. Forhold som ikke tas tilstrekkelig hensyn til i forbindelse med øvelser, vil med stor sannsynlighet heller ikke fungere i en reell krisesituasjon.

Verdivurdering av informasjonen blir ofte ikke godt nok ivaretatt i forbindelse med øvelser. Summen av dette er at sikker informasjonsflyt under en krisehåndtering blir utilfredsstillende. Rask og målrettet informasjonsflyt er en suksessfaktor for å utøve en effektiv kriseledelse. Resultatet av mangler i evnen til å kommunisere sikkert på tvers, gjør det vanskelig å etablere et felles situasjonsbilde, noe som ofte er avgjørende under en krisehåndtering. Sikkerhetsmessige mangler tilliggende øvelsesaktivitet er ikke av ny dato. Av den grunn synes det som om de sikkerhetsmessige sidene i for liten grad er en del av evalueringen av øvelsene.

Som de fleste andre lover er også sikkerhetsloven primært ment for fredstid. For å kunne forberede hvilke standarder som skal gjelde for informasjonssikkerhet i krise og krig må det gjøres et forarbeid i fredstid. Av forarbeidene til sikkerhetsloven går det implisitt frem at det må foreligge en vurdering av, eller plan for, ivaretakelse av informasjonssikkerhet i krise eller krig.

Sikkerhetsgraderte anskaffelser

Norske bedrifter spiller en viktig rolle i vårt nasjonale sikkerhetsarbeid. Dette gjelder ikke minst for bedrifter som faller inn under sikkerhetsloven fordi de håndterer sikkerhetsgradert informasjon. Offentlig forvaltning kan dra lærdom av hvordan flere bedrifter faktisk organiserer og administrerer sikkerhetsarbeidet. Det er flere forklaringer på det høye

sikkerhetsfokuset hos leverandørene. Omdømme og tillit i markedet er viktig for konkurransekraften. Mangelfull sikkerhetskultur vil kunne få direkte konsekvens for bunnlinjen. Videre avhenger tildeling av sikkerhetsgraderte oppdrag av troverdighet på sikkerhetssiden. En ytterligere årsak til at sikkerhetsarbeidet blant private leverandører jevnt over er tilfredsstillende, er NSMs og anskaffende myndigheters regelmessige tilsynsaktivitet. Praksisen med inngåelse av sikkerhetsavtaler mellom anskaffelsesmyndighet og leverandør etablerer gjensidige forpliktelser bidrar også til at sikkerhetsarbeidet ivaretas på en god måte. I de tilfeller hvor NSM finner mangler ved sikkerhetsarbeidet hos aktuelle leverandører, fremstår ofte mangelfull forankring hos ledelsen som en vanlig årsak. NSM vil understreke behovet for at sikkerhetsbehovene inkluderes så tidlig som mulig i aktuelle prosjekter. Et tidlig fokus vil både ivareta sikkerheten og gi best utnyttelse av samfunnets og bedriftenes ressurser.

Informasjonssikkerhet og internasjonale forpliktelser

Norge er en del av et omfattende internasjonalt samarbeid hvor sikkerhetsgradert informasjon utveksles. Utveksling av sensitiv informasjon er viktig for å ivareta våre overordnede strategiske sikkerhetsinteresser. For deler av industrien er formalisert mellomstatlig utveksling av sensitiv informasjon avgjørende for å kunne delta i konkurransen om graderte leveranser. Et annet forhold som har bidratt til mer utveksling av sikkerhetsgradert informasjon er forebygging av terror. NSM spiller en viktig rolle i tilretteleggingen for at Norge skal kunne utveksle gradert informasjon med utlandet.

Både sivile og militære norske myndigheter utveksler til dels høyt gradert informasjon med NATO. Det forventes at sikkerhetsgradert informasjonsutveksling med EU vil øke. En egen sikkerhetsavtale mellom Norge og EU gjør det mulig å utveksle gradert informasjon. Vår deltagelse i EUs *Battle Groups* og i Galileo-prosjektet er allerede realiserte ordninger. Et tredje eksempel er at EU ønsker å inngå i fremtidige NATO-øvelser, hvilket igjen innebærer at Norge og EU sannsynligvis vil utveksle gradert informasjon. I Soria Moria-erklæringen uttaler regjeringen at den vil arbeide for et styrket FN, og øke den norske deltakelsen sivilt og militært i FN-operasjoner. I slike operasjoner antas det å bli behov for å kunne utveksle skjermingsverdig informasjon med FN, og de land som stiller med styrkebidrag.

Norge utveksler informasjon bilateralt med en rekke nasjoner. Til grunn for den graderte informasjonsutvekslingen ligger det bilaterale sikkerhetsavtaler. I dagens globaliserte

samfunn er behovet for slike avtaler økende. Internasjonalt samarbeid som nødvendiggjør utveksling av sikkerhetsgradert informasjon er ikke lenger bare et militært fenomen, men gjør seg gjeldende på stadig nye samfunnsområder, blant annet innen luftfarts-, sjøfarts- og justissektoren. Sikkerhetsavtaler er også nødvendig for at norsk industri skal kunne konkurrere om sikkerhetsgraderte oppdrag i andre nasjoner.

Dersom norske virksomheter ikke beskytter andre lands eller internasjonale organisasjoners informasjon på en tilfredsstillende måte, vil dette kunne svekke begge parters sikkerhet. Det fremstår derfor som viktig at norske virksomheter følger de krav som stilles med tanke på håndtering av samarbeidende aktørers informasjon.

Personellsikkerhet

Før tilgang til skjermingsverdig informasjon gis skal personellet være sikkerhetsklarert og autorisert. Autorisasjon skjer lokalt ved virksomheten som skal gi vedkommende tilgang til informasjonen. Autorisasjonens formål er å forsikre seg om at regelverket og eget sikkerhetsansvar er forstått, i tillegg til å etablere et tillitsforhold. NSM har i tidligere risikovurderinger pekt på betydelige mangler tilknyttet gjennomføring av autorisasjon. NSM har derfor i 2006 lansert *Håndbok i autorisasjon og autorisasjonssamtale.*

Kostnader tilknyttet sikkerhetsbrudd

Ofte er det en langvarig prosess å få på plass nødvendige sikkerhetstiltak. Ikke minst omfatter dette utarbeidelse og operasjonalisering av beredskapsplanverk. Vår motstandsdyktighet mot sikkerhetstruende hendelser reduseres dersom slike planverk ikke omgis av et velfungerende sikkerhetsregime. Kostnader tilknyttet brudd på sikkerheten kan vurderes på ulike måter. Sikkerhetsgradert informasjon i hendene på en motstander vil kunne innebære redusert sikkerhet. En annen type kostnader i forbindelse med sikkerhetsbrudd kan være behovet for nødvendige utbedringer. En tredje kategori kostnad ved sikkerhetsbrudd vil være tap av tillit og omdømme.

NSM vil advare mot at virksomheter i frykt for ekstrautgifter unnlater å rapportere grove sikkerhetsbrudd. Skadefølgene kan forverres dersom de ikke blir håndtert så fort som mulig. Samtidig vil følgeskader ikke bli unngått eller skadens omfang bli erkjent. Videre har virksomhetene et ansvar for å varsle andre virksomheter som sikkerhetsbruddet har

betydning for. I tillegg kommer rapporteringsplikten til NSM og om nødvendig en anmeldelse til politiet.

Foto- og kartkontroll

NSM driver myndighetsutøvelse med utgangspunkt i Lov om forsvarshemmeligheter. Med hjemmel i loven ble den underliggende forskriften om foto- og kartkontroll sist oppdatert i 1997. Den heter Forskrift om fotografering mv fra luften og kontroll av luftfotografier og opptaksmateriale fra luftbårne sensorsystemer. Hensikten med forskriftens bestemmelser er, gjennom utelatelse eller retusjering av objekter på bilder og offentlige kart og kontroll med luftfotografering, å skjerme forsvarsviktige installasjoner mot spionasje.

En utfordring med lov og forskrift er at de ikke fanger opp sivile behov for skjerming. Sett i lys av at sivil kritisk infrastruktur er av betydning i krise og krig fremstår dette som en sårbarhet. Nedrustiningsavtaler og initiativer for tillitsskaping, som *Open Skies,* har gjort det lettere for andre nasjoner å overfly og fotografere skjermingsverdige objekter. Et forhold som har gjort etterretningsinnhenting enklere er opphevelsen av fotoforbudet for passasjerer i rute-, charter- eller taxifly over militære flyplasser. Forbudet ble opphevet på 1990-tallet. Satellittfoto blir stadig mer nøyaktig. De satellitter som fremmed etterretningstjeneste styrer eller har tilgang til anses å være svært gode, og forskjellen på opptaksmaterialet mellom disse og det som kommer fra lavtflyvende fotoaktivitet blir stadig mindre.

Tilgang til satellittfoto via Internett har økt mulighetene for etterretningsinnhenting. Et konkret eksempel er den amerikanske tjenesten *Google Earth*. Detaljeringsgraden, brukervennligheten samt mulighet for å koble sammen informasjon, gjør gratis foto- og karttjenester på Internett til underholdende og nyttige geografiske informasjonssystemer (GIS). Bruksområdene er mange og tilgjengeligheten er høy. Dette gir samtidig en rekke utfordringer med hensyn å beskytte skjermingsverdig informasjon. Slike tjenester er i rask utvikling. Det er likevel mulig å komme med relevante tiltak. Et problem er utilstrekkelig regelverk for sivile formål.

Kartproduksjonen er i stor grad er digitalisert. Samtidig legges stadig mer informasjon inn i kartene. Etableringen av Norge digitalt i januar 2005 er viktig i denne sammenheng. De ordninger som dagens regelverk legger opp til når det gjelder kartkontroll, treffer ikke riktig som en følge av endringer i produksjonsprosessene for kart. Mye av produksjonen,

eksempelvis lokalt i kommunene, omfattes ikke. Informasjonsskjermingen blir følgelig ikke effektiv.

NSM har på denne bakgrunn foreslått at det gjennomføres en revisjon av dagens regelverk. Det er etter NSMs mening viktig å ta gjennomtenkte skritt i denne prosessen. Åpenhet på dette området (objekter og geografisk informasjon) vil medføre publisering ved hjelp av Internett. Informasjon lagt på nettet kan for alle praktiske formål ikke trekkes tilbake.

Lov om forsvarshemmeligheter § 3 fastsetter at det kreves samtykke fra Kongen for å foreta andre målinger av havbunnen enn det som er nødvendig for sikker navigasjon. Bestemmelsen er operasjonalisert i Forsvarssjefens navigasjonsplan. Etter denne planen er detaljerte dybdedata å anse som sikkerhetsgradert informasjon, og er følgelig ikke allment tilgjengelig. Dette system møter i dag betydelige faktiske utfordringer. En rekke virksomheter har i dag et legalt behov for tilgang til nøyaktige dybdedata. Eksempler er fiskeoppdrett og legging av kabler og rørledninger på havbunnen. Kriteriene for frigivelse av nøyaktige dybdedata fremstår i dag som til dels uklare og til dels lite tilpasset samfunnets behov.

NorCERT– status og utviklingstrender

NorCERT (*Norwegian Computer Emergency Response Team*) under NSM er et nasjonalt senter for håndtering av alvorlige dataangrep mot kritiske infrastrukturer, samfunnsfunksjoner og informasjonssystemer. NorCERT skal forebygge mot og reagere på internettangrep, og være nasjonale kontakt- og koordineringspunkt internasjonalt. NorCERT har dermed en unik oversikt over sikkerhetssituasjonen i samfunnskritisk IKT-infrastruktur, og har til enhver tid et oppdatert trusselbilde for Internett. NorCERT er delvis privatfinansiert.

NorCERT har tett samarbeid med blant andre NorSIS, Datakrimavdelingen i Kripos, store nasjonale industrikonsern, Forsvarets forskningsinstitutt, internettleverandører (ISPer), britiske *National Infrastructure Security Co-ordination Centre* (NISCC) og *NATO Computer Incident Respons Center* (CIRC). I tillegg er vi medlem av *Forum for Incident Response and Security Teams* (FIRST), *European Government CERT Group* (EGC), *International Watch and Warning Network* (IWWN) og Nordisk CERT-Forum (NCF).

Varslingssystem for digital infrastruktur (VDI) er en seksjon i NorCERT, og opererer et sensorsystem som samler inn nettverksdata ved hjelp av *Intrusion Detection System* (IDS) sensorer. Deltagerne som leverer data til VDI er representanter for kritisk digital infrastruktur i Norge. De fleste deltagerne har mange datasystemer som er eksponert mot Internett, men har generelt gode sikkerhetsmekanismer sammenlignet med gjennomsnittet av systemer

tilknyttet nettet. Dersom flere av deltagerne blir angrepet samtidig, kan dette få konsekvenser for den nasjonale sikkerheten. Ved å sammenstille dataene fra VDI-sensorene med data fra åpne og lukkede kilder, både nasjonale og internasjonale, forsøker NorCERT å forutsi sannsynligheten for angrep.

Trusler

Botnett eller botnettverk er fagterminologi for en samling av kompromitterte maskiner som opererer sammen i ett nettverk. Maskinene er infisert med et ondsinnet program som kobler seg opp mot et kommandosenter, hvilket gjør det enkelt å administrere hele botnettet. På verdensbasis finnes det i dag tusenvis av botnettverk som opereres av forskjellige aktører. Botnett benyttes i økende grad til å oppnå økonomisk vinning. Økt fokus på økonomi har gjort det viktigere for kriminelle å unngå deteksjon. Dette gjøres ved å dele opp botnettverkene i mindre, men samtidig mer robuste enheter. Tidligere var det vanligere at botnettverk kunne bestå av over en million kompromitterte maskiner. Det brukes i tillegg mer ressurser på å kamuflere at maskiner er infisert, og trusselaktørene benytter stadig mer avansert teknologi, herunder kryptering, for ikke å bli avslørt.

Et tjenestenektangrep har som formål å angripe en tjeneste slik at denne ikke lenger fungerer. På Internett kan dette gjøres ved å sende store mengder datatrafikk mot et bestemt mål. Det blir kø og opphopning i nettverket, og tjenesten blir utilgjengelig for omverdenen. På engelsk brukes begrepet *Denial of Service* (DOS), eller *Distributed Denial of Service* (DDoS) dersom angrepet er distribuert. Distribuert vil si at trafikken som sendes er generert fra flere maskiner samtidig.

Utsatte mål er nettbutikker, auksjonssider og online spillsider samt andre som til enhver tid er avhengig av Internett for å tilby sine tjenester. I inneværende år er det observert en økt bruk av tjenestenekt i forbindelse med politiske eller religiøse konflikter. Etter trykkingen av Muhammed-tegningene, ble flere hundre danske nettsider angrepet. Tjenestenektangrep ble her benyttet for å forsøke å lamme danske aktører på Internett. I Sverige gikk det svenske politiet til aksjon mot nettstedet *The Pirate Bay@,* en katalog over fildelingsressurser. Etter politiaksjonen ble nettsidene til det svenske politiet utsatt for tjenestenektangrep.

Et ytterligere utviklingstrekk tilknyttet Internett er at aktører som politi og anti-virus selskaper har blitt mer attraktive mål for kriminelle. Resultatet blir dermed at de i større grad enn tidligere må forsvare seg, i tillegg til å etterforske og utarbeide programvare.

Phishing er forsøk fra en tredjepart på å lure et individ, en gruppe, eller en organisasjon til å gi fra seg sensitiv informasjon. Denne informasjonen kan deretter misbrukes, og hensikten er

i økende grad økonomisk vinningskriminalitet. *The Anti-Phishing Working Group* (APWG) rapporterer at antall phishingsider inneværende år er fordoblet i forhold til 2005. Mer enn 90 prosent av alle phishingforsøk retter seg mot finansielle institusjoner, men det foreligger også eksempler på at slike angrep retter seg mot andre virksomheter. Svindelforsøkene blir stadig mer målrettede og de tilpasses mindre grupper. NorCERT kontaktes jevnlig angående phishingangrep. Nye teknikker og verktøy bidrar til å gjøre risikoen for phishingangrep vedvarende og bekjempelsen av slike angrep er nå mer komplisert.

Det har i en lengre periode blitt observert økende ondsinnet aktivitet fra målrettede trojanere. Angrepene inkluderer både omfattende kartleggingsaktivitet samt målrettede angrep mot spesifikke vestlige virksomheter og myndigheter. Angrepsmetoden er i mange tilfeller e-post. E-postene er forfalsket og inneholder informasjon som ved første øyekast virker autentisk og viktig. Idet vedlegget åpnes, benyttes automatiske metoder for å installere et ondsinnet program. Det ondsinnede programmet skjuler sin tilstedeværelse på maskinen samtidig som det fanger opp brukerens passord og brukernavn I tillegg forsøker programmet å sende ut sensitive dokumenter og annen informasjon som finnes i datamaskinen. Norske virksomheter fremstår som et klart mål for utenlandsk industrispionasje over Internett.

Organiserte kriminelle utnytter stadig oftere og i økende grad teknologi for økt økonomisk vinning. Det er ulike måter å tjene penger på; herunder phishing, spam, kredittkort tyveri, identitetstyveri, utpressing og installering av uønsket reklame som det mest vanlige. Et unikt verktøy for å utføre disse handlingene er botnett, og mye av undergrunnsøkonomien handler om utleie, salg og kjøp av botnett, eller dets tjenester.

Trender

Det er registrert en sterk økning i bruk av botnett for økonomisk vinning. Fra å ha en ganske snever målsetning, slik som tjenestenektangrep, masseutsendelse av e-post (spam) og distribuering av ulovlig materiale benyttes botnettinfiserte maskiner i dag til mer avanserte former for datakriminalitet, for eksempel være tjenesteleverandør for phishingsider som kan flytte siden fra maskin til maskin for å unngå at den blir stengt ned. Myndigheter i mange land evner ofte ikke å handle raskt nok. Dette utnyttes av kriminelle til å svindle til seg penger eller informasjon. Et forbedret sikkerhetsnivå i dagens operativsystemer gjør at realverdien til en kompromittert maskin øker. Det legges derfor også mer arbeid i å kamuflere den ondsinnede koden for å unngå deteksjon fra antivirusprogramvare og andre sikkerhetsmekanismer.

Virus, ormer, trojanere og annen uønsket programvare som installeres i datamaskiner uten samtykke kalles ondsinnet programvare. En kjent fagterminologi for dette er *malicious software*, gjerne forkortet til *malware*. NorCERT ser en kraftig økning av antall ondsinnet

kode som blir spredd, og tallene øker for hver måned. De fleste stoler på at antivirusprogramvare stopper alt og er ikke forberedt på å håndtere en situasjon der datamaskiner blir infisert med ukjent ondsinnet kode.

NorCERT– egne observasjoner

I tillegg til å sammenstille data fra åpne og lukkede kilder både nasjonalt og internasjonalt, samler NorCERT også inn egne data gjennom et nettverk av IDS-sensorer. Dette er organisert gjennom VDI-varslingssystem som også er en del av NorCERT. Deltagerne i sensornettverket er representanter for kritisk digital infrastruktur i Norge og har utplassert sensorer i sine datanettverk for innsamling av informasjon.

VDI-pulsen er delt opp i 5 nivåer og er kort forklart i tabellen under.

Pulsnivå	Betydning
1	Ingen kjent fare for kritisk digital infrastruktur.
2	Moderat fare for kritisk digital infrastruktur.
3	Overhengende fare for vellykkede angrep rettet mot kritisk digital
4	Stor fare for at store deler av kritisk digital infrastruktur vil bli satt ut av
5	Store deler av kritisk digital infrastruktur er satt ut av spill.

Tabell 1 (U) Kort forklaring av de forskjellige nivåene i VDI-pulsen.

I perioden fra september 2005 til september 2006 har det vært i alt fem pulsøkninger. Tirsdag 11. oktober ble VDI-pulsen hevet til nivå 2 på grunn av tre kritiske sårbarheter annonsert av Microsoft. De to mest kritiske sårbarhetene kan tillate en angriper å få fullstendig kontroll over en maskin som er sårbar. Torsdag 3. november ble VDI-pulsen hevet til nivå 2 på grunn av publisert informasjon om at Cisco IOS inneholder en sårbarhet som kunne muliggjøre at en ikke-autentisert angriper fikk kjørt vilkårlig kode. Et vellykket angrep kan da resultere i full kompromittering. VDI-pulsen ble økt til nivå 2 den 10. januar 2006 som følge av en sårbarhet i nyere versjoner av Outlook, Exchange og Office. Tirsdag 9. mai offentliggjorde Microsoft blant annet en alvorlig sårbarhet knyttet til behandlingen av kalendervedlegg i Microsoft Exchange Server. Sårbarheten kunne resultere i full kompromittering av systemet, og ble av NorCERT vurdert som svært kritisk. Pulsen ble derfor hevet til nivå 2. Torsdag 3. august 2006 ble VDI-pulsen hevet til nivå 2 på grunn informasjon om en sårbarhet i drivere til trådløse nettverkskort. Sårbarhetens natur gjør at den ikke oppdages av verken brannmur eller antivirusprogrammer, og sårbarheten kan brukes i en orm. Sårbarheten gir mulighet for eksekvering av vilkårlig kode og ingen autentisering for tilgang er nødvendig.

Den fremtredende nedgangen i helgene er en trend VDI har registrert så lenge sensorene har vært utplassert. En teori på dette er at mange angrepsforsøk blir utført fra kompromitterte

maskiner, og ofte av automatisert kode. Når folk går fra jobb på fredag, stenger de ofte arbeidsmaskinen sin, og på den måten blir det færre kompromitterte maskiner tilgjengelig på Internett.

Noen av NSMs anbefalinger

Det bør vurderes hvorvidt sikkerhetsloven bør omfatte flere relevante virksomheter innen sentrale samfunnssektorer som olje- og gassektoren, finanssektoren, IKT-sektoren, helsesektoren, samferdselssektoren, kraftsektoren, elektronisk kommunikasjon og satellittbasert infrastruktur.

Et stadig tettere sikkerhetssamarbeid med EU er sannsynlig. Norsk deltagelse i *Battle Groups* og felles krisehåndteringsøvelser er to konkrete eksempler. Det bør ses nærmere på videreutvikling av sikkerhetssamarbeidet med EU.

NSM anbefaler at Nødnettet gjøres så robust som mulig. En gjennomtenkt sikkerhetsadministrasjon rundt Nødnettet fremstår som avgjørende. Det er viktig at administrative sikkerhetstiltak utarbeides så tidlig som mulig og kan implementeres etter hvert som systemet gradvis tas i bruk.

Internettleverandører bør pålegges å implementere tiltak for å motvirke at norske datamaskiner blir brukt i angrep mot norske eller internasjonale mål. Erfaring tilsier at slike tiltak ikke blir iverksatt uten at myndighetene stiller krav. En slik bestemmelse vil være et viktig tiltak for å ansvarliggjøre bransjen.

Sikkerhetsbrudd vil kunne medføre økonomiske utgifter og ikke-økonomiske tap. Alle virksomheter bør ha innarbeidede rutiner for rask håndtering av sikkerhetsbrudd. Rask håndtering vil bidra til å gjenopprette sikkerheten før skadefølgene blir større, samt bidra til å begrense utgifter til gjenopprettelse. Alle virksomheter som utveksler sikkerhetsgradert informasjon internasjonalt bør gjennomgå egen praksis rundt hvordan utenlandsk informasjonen beskyttes.

En systematisk sammenstilling av åpen informasjon med et høyt detaljeringsnivå, satt sammen i store databaser eller nettløsninger, må gjøres til gjenstand for en grundig verdivurdering av hensyn til rikets sikkerhet og vitale nasjonale sikkerhetsinteresser. Den som forestår sammenstillingen av informasjonen har ansvaret for å foreta verdivurderingen av den samlede informasjonen. Det er særlig viktig at det foretas en verdivurdering av bygg, prosjekter, databaser og nettsteder i en tidlig fase. Det anbefales at ledelsen i alle

virksomheter underlagt sikkerhetsloven vektlegger verdivurdering. De enkelte departementene bør utarbeide interne retningslinjer for verdivurdering innen sine respektive myndighetsområder. NSM har utarbeidet en overordnet veiledning i verdivurdering og vil prioritere råd, veiledning og undervisning tilknyttet verdivurdering. NSM vil ta initiativ til et samarbeid med Statens kartverk, som innebærer at skjermingsbehovet knyttet til informasjon som gjøres tilgjengelig innenfor samarbeidsmodellen Norge digitalt, blir vurdert i henhold til sikkerhetsloven.

IKT-sikkerheten bør prioriteres i aktuelle virksomheter. Ledelsesforankring er her viktig. Lederne må legge til rette for at datasikkerhetsleder får opplæring i sikkerhetsgodkjenning og sørge for oppfølging av IKT-sikkerheten. Flere virksomheter bør gjennomgå egne rutiner for bruk av maskinlesbare lagringsmedia, herunder minnepinner.

NorCERTs målgruppe er virksomheter med kritiske infrastrukturer, samfunnsfunksjoner og informasjon.

- Slike virksomheter bør etablere gode rutiner og prosedyrer for rask testing og utrulling av programvareoppdateringer. Det er viktig å innlemme både nettverkskomponenter og tjenesteprogramvare i disse rutinene, og ikke kun konsentrere seg rundt operativsystemer som det har vært mest sårbarhetsfokus på de siste årene.
- Virksomhetene bør skaffe seg oversikt over hvor avhengig de er av Internett. Krav til sikkerhet, oppfølging ved angrep, deteksjons- og reaksjonsverktøy og metoder bør avtalefestes med internettleverandør.
- Virksomhetene bør, med utgangspunkt i jevnlige risikoanalyser, utforme beredskaps og krisehåndteringsplaner for å forebygge og håndtere uønskede IKT-hendelser. Planverkene må øves for å gjøre organisasjonen forberedt på å håndtere en krise. Det er viktig at virksomhetene kjenner til sitt nærmeste CERT-kontaktpunkt, slik at ansvarlige myndigheter kan holdes oppdatert.
- Virksomheter innenfor samme bransje bør opprette samarbeid innenfor sikkerhetsarbeid og hendelseshåndtering. Samarbeid øker kapasiteten til å reagere og vil gjøre virksomhetene bedre rustet til å håndtere IKT-hendelser.
- Aktuelle virksomheter bør informere NorCERT ved alvorlige IKT-hendelser mot kritiske infrastrukturer, samfunnsfunksjoner og informasjon.

NSM mener det foreligger et behov for større nasjonale øvelser med utgangspunkt i IKT-kriser. En nasjonal cyberøvelse vil kunne gi nyttige erfaringer om krisehåndteringen ved større sikkerhetsmessige hendelser på Internett. Øvelser er viktig for å avdekke personell- og

kompetansemangler, samt mangel på informasjonsflyt mellom private virksomheter og offentlig forvaltning. I tillegg vil slike øvelser være viktige for å bygge relasjoner internt i hver organisasjon og mot samarbeidspartnere. En nasjonal cyberøvelse vil bidra til at vårt nasjonale kriseapparat er forberedt på at cyberkriser kan oppstå. NorCERT vil utarbeide et konsept for hvordan en slik øvelse kan gjennomføres nasjonalt.