NSMs risikovurdering 2005, UGRADERT versjon

1 Innledning

NSM er pålagt av Forsvarsdepartementet og Justis- og politidepartementet å rapportere om risikobildet og sikkerhetstilstanden. Rapportering skjer blant annet gjennom NSMs risikovurdering. Risikovurderingen er sikkerhetsgradert og distribueres årlig til departement, Forsvaret, fylkesmenn og andre virksomheter som omfattes av lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). For en mer omfattende beskrivelse av forebyggende sikkerhetstjeneste og metodikk knyttet til NSMs overordnede risikovurdering, vises det til tidligere utgitte risikovurderinger for 2003 og 2004.

Risikovurderingen har tre hovedmål:

1. Gi et innblikk i dagens risikobilde.
2. Presentere informasjon om sikkerhetstilstanden.
3. Vurdere sikkerhetstilstanden opp mot risikobildet og fremme anbefalinger om tiltak.

2 Risikobildet

Faktorene sikkerhetsmessig verdi, sikkerhetstrussel og sårbarhet utgjør til sammen risikobildet. Kjennskap til alle faktorene i risikobildet er en forutsetning for å være i stand til å innrette defensive, forebyggende sikkerhetstiltak mot spionasje, sabotasje og terrorhandlinger på en hensiktsmessig måte.

2.1 Sikkerhetsmessig verdi

Hva er det som har sikkerhetsmessig verdi? I sikkerhetsloven heter det at informasjon og objekter av betydning for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser har sikkerhetsmessig verdi. Territoriell integritet har vært hovedinnholdet i begrepet *rikets sikkerhet.* Dette er endret nå, blant annet med bakgrunn i et endret trusselbilde hvor en forsøker å bekjempe såkalte asymmetriske aktører, det vil si terrorister, langt unna statsterritoriet til de land som kanskje er hovedmålet for terrorhandlingene.

Vitale nasjonale sikkerhetsinteresser omfatter kritisk infrastruktur innenfor vitale samfunnsfunksjoner som energi- og matforsyning, samferdsel, telekommunikasjon, helseberedskap samt bank- og pengevesen. Opplistingen er ikke uttømmende.

Et sentralt spørsmål når det gjelder å vurdere om egen informasjon er skjermingsverdig (altså at den har sikkerhetsmessig verdi) i henhold til sikkerhetsloven, må være om informasjonen i vesentlig grad kan misbrukes slik at virksomheten selv eller andre virksomheter rammes. Et annet spørsmål vil være om sammenstillingen av ugradert informasjon kan utgjøre en så verdifull kunnskapsbase for mulige ondsinnede aktører, at den helhetlige informasjonen vil kunne være skjermingsverdig i henhold til sikkerhetsloven.

Det er også viktig at virksomhetene er i stand til å vurdere konsekvenser for egen sikkerhet og oppgaveløsning dersom en skulle rammes av terror, sabotasje eller spionasje samtidig som en ser egen virksomhet i en større sammenheng. Et viktig spørsmål som virksomheter bør være i stand til å besvare er hva som er *mest* kritisk for at oppgaveløsningen skal kunne fortsette. Det er neppe mulig å beskytte alt. Derfor er det avgjørende å kunne foreta en analyse som kartlegger det virksomhetskritiske hvor også samfunnsmessige og nasjonale konsekvenser inngår i analysen.

2.2 Sikkerhetstrusselen

Spionasjetrusselen[1] eksisterer fremdeles i form av tradisjonell, statsinitiert spionasje. Terroraktører må også innhente informasjon for å kunne gjennomføre terrorhandlinger. Forsvaret, industri, politiske beslutningsprosesser, sårbare punkter i samfunnet og teknologi er blant de **mål** som er attraktive i forhold til innhenting av informasjon ved bruk av fordekte midler (spionasje).

Eksempler fra andre land viser at fremmed etterretning ofte arbeider gammeldags, med verving som en mye brukt **metode**. På generell basis kan det sies at det finnes et mangfold av metoder for å utføre spionasje. Ny teknologi gir nye muligheter for spionasje. Samtidig gir også teknologi nye muligheter for forebygging.

[1] Sikkerhetsloven § 3 nr. 3: ”Spionasje; innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt.”

Informasjon om planlagte og utførte *terrorhandlinger*[2] i Europa kan si noe om utviklingstrekk i forhold til mål og metode.

Spania ble rammet av en terroraksjon 11. mars 2004. Det har også blitt avverget flere planlagte terroraksjoner i Europa siden år 2000. Det er gjennomgående radikale, islamistiske grupperinger som står bak planene. **Målutvelgelsen** er variert og omfatter symbolske, militære, statlige og private mål. Finansinstitusjoner synes også å være attraktive mål. Eksplosiver dominerer fremdeles som **metode,** blant annet i form av sprengstoffet C4. Sprengstoff i form av ammoniumnitrat blandet med for eksempel diesel synes også å være en aktuell metode.

Avslørte aksjonsplaner synes å indikere at terrorgrupperinger er interessert i å kunne produsere giftstoffer. Men selv om intensjonen ser ut til å ligge på et jevnt høyt nivå, ser det foreløpig ikke ut som om kapasiteten til å produsere og spre blant annet giftstoffer i større mengder er til stede hos terrorgrupperinger.

2.3 Sårbarhet

Den tredje og siste komponenten i risikobildet er sårbarhet. Sårbarhet er svakheter som reduserer eller begrenser evnen i et system eller i samfunnet til å motstå uønskede, negative hendelser. I denne sammenheng manifesterer hendelsene seg i første rekke som spionasje, sabotasje eller terror[3].

Samfunnets avhengighet av teknologi kan føre til økt sårbarhet. Nedenfor beskrives kort noen eksempler på dette.

Internett har etter hvert fått stor verdi for samfunnet. Stadig flere tjenester, både offentlige og private, baserer seg på bruk av Internett. Internett er et system som i utgangspunktet var designet nettopp for å være robust og redundant, slik at mulighetene for å utføre sabotasje mot Internett skulle være små. I dag er situasjonen på mange måter annerledes, blant annet fordi mange aktører ønsker å tjene penger på folks bruk av Internett. Dette innebærer at trafikken må styres via enkelte punkter for at registrering av trafikk skal kunne skje. En konsekvens er at enkeltpunkter i Internettsystemet har fått større betydning enn tidligere. Dette gjør Internett mer

[2] Sikkerhetsloven § 3 nr.5: ”Terrorhandlinger; ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål.”

sårbart både overfor logiske angrep i form av for eksempel tjenestenektsangrep, men også overfor klassiske angrep i form av *sabotasje*[4] rettet mot nøkkelpunkter.

Samfunnets avhengighet av navigasjonssystemer som GPS, øker. Eksempler på bruksområder er innen alle deler av transportsektoren, energisektoren, telekommunikasjon, finanssektoren, fiskerisektoren, miljøsektoren, nødetatene og militærsektoren. GPS har ulike svakheter eller sårbare områder. Andre radiotjenester, for eksempel innenfor VHF-båndet, kan gi forstyrrelser som kan medføre interferens og påfølgende unøyaktighet eller manglende evne til å ta imot signaler fra satellitter. Bruk av jammeutstyr kan også være en utfordring. De fleste militærvesen har kraftig jammeutstyr, gjerne montert på fly, som kan sette GPS-signalene ut av funksjon over store områder. Samtidig er jammeutstyr også kommersielt tilgjengelig. I tillegg er utstyr som sender ut villedende signaler en sikkerhetsmessig utfordring.

Galileo er et europeisk alternativ til GPS som er under utvikling nå. Navigasjonssystemene vil være interoperable. To uavhengige navigasjonssystemer kan gi betydelig redundans og minske sårbarheten.

Sårbarheten knyttet til elektroniske informasjonssystemer blir stadig større. En årsak til økt sårbarhet er at det stilles store krav til mobilitet. Begrepet mobilitet kan dekke områder som trådløs teknologi, mobiltelefoner, PDA (Personal Digital Assistant), bærbar PC og så videre.

Bruk av trådløst nettverk etter 802.11 standarden, såkalt WLAN (Wireless Local Area Network), har blitt svært populært både blant hjemmebrukere og bedrifter. Dagens standard omfatter to krypteringsprotokoller; WEP (Wired Equivalent Privacy) og WPA (Wi-Fi Protected Access). WPA er regnet for å være den minst svake. I WEP-protokollen har det blitt avslørt en rekke kryptografiske svakheter som gjør det enkelt for uvedkommende å knekke krypteringen. Programvare for å gjøre dette kan lastes ned fra Internett. Gjennom media har det for øvrig blitt satt søkelys på institusjoner som benytter trådløse nettverk uten noen form for kryptering. Dette gjør at nettverket ligger helt åpent for uvedkommende.

---

[3] Teknisk og menneskelig svikt samt naturskade kan også lede til sikkerhetsbrudd og kompromitteringer. Dette viser blant annet at sammenhengen mellom tilsiktede og utilsiktede hendelser kan være sterk i forhold til forebyggende sikkerhetstjeneste fordi konsekvenser av hendelsene kan være de samme.

Mobiltelefoner i GSM-nettet kan avlyttes. Mobiltelefoner kan også manipuleres. En manipulering kan føre til at det blir mulig for utenforstående å benytte mobiltelefonen som et medium for avlytting av sensitiv informasjon.

PDA og minnepinner (memory sticks) har etter hvert fått stor lagringskapasitet og kapasiteten er stadig økende. Relativt store mengder informasjon kan tas med ut av det kontrollerbare området til virksomhetene. Fysisk sikring av små, flyttbare enheter innebærer en stor utfordring. En PDA kan inneholde informasjon som gir tilgang til virksomhetens nettverk.

Elektroniske informasjonssystemer består generelt av stadig flere komponenter som fører til en kompleks konfigurasjon og administrasjon. Stadig integrering av systemer og produkter fordi det oppstår nye ønsker om hva systemet faktisk skal kunne gjøre kan også medføre økt sårbarhet. Integreringen fører til at en har varierende kontroll med de nye produktene når det gjelder muligheter for skjulte feil og mangler. Sårbarheten kan forsterkes ved omstillinger. Det er derfor viktig å ha fokus på kompetanse hos personellet som skal operere systemene.

NSM utarbeider veiledninger for mange teknologier som skal sikre en forsvarlig konfigurering og bruk av informasjonssystemet. NSM forsker også, blant annet på prototyper, for å få kjennskap til hvor god sikkerheten i nye teknologier og produkter faktisk er.

3 Sikkerhetstilstanden

NSMs grunnlag for å kunne uttale seg om sikkerhetstilstanden er erfaringer fra tilsyn, resultater fra en spørreundersøkelse i regi av NSM, innrapporterte hendelser, innhenting av informasjon fra samarbeidende tjenester og ulike fagmiljøer samt medieovervåkning.

Verdivurdering

Resultater fra spørreundersøkelsen viser blant annet at virksomhetenes egen, tidligere praksis har en viss betydning for vurderingen av hvilket nivå sikkerhetsgraderingen skal settes til. Dette kan bety at det er problematisk for virksomhetene å endre sin praksis i tråd med endringer i risikobildet. Dette kan igjen føre til at informasjon som burde ha blitt beskyttet ikke blir beskyttet, eller at virksomheter bruker unødige ressurser på å beskytte informasjon som ikke er spesielt verdifull.

---

[4] Sikkerhetsloven § 3 nr. 4: ”Sabotasje; tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet, eller tilsiktet uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering.”

Implementering av sikkerhetsloven med forskrifter

Resultater fra spørreundersøkelsen viser at virksomhetene ikke ser ut til å evaluere egne sikkerhetstiltak i særlig grad. Dette innebærer at virksomhetene egentlig ikke vet om tiltakene gir den sikkerhet de er ment å skulle gi.

Gjennomføring av autorisasjonsprosessen er det andre området som har spesielt forbedringspotensial. Flere virksomheter gjennomfører ikke autorisasjonsprosessen. Autorisasjon er et sikkerhetstiltak som skal sikre at den sikkerhetsklarerte har tilstrekkelig kunnskap om håndtering av skjermingsverdig informasjon.

Tilsynserfaringer viser at sikkerhetsorganisasjonen ofte nedprioriteres i en omstillingsfase. Dette kan føre til at de forebyggende sikkerhetstiltakene som sikkerhetsloven med forskrifter angir ikke blir implementert grunnet kapasitetsproblemer hos personellet.

Svakheter ved regelverk og organisering

Regelverket synes å ha noen svakheter i forhold til å kunne forebygge sikkerhetstruende virksomhet. Forebyggende sikring av kritisk infrastruktur mot for eksempel terrorhandlinger kan bedres ved at sikkerhetsloven gis anvendelse på flere virksomheter, som er viktige for samfunnet, enn i dag. Dette kan spesielt være aktuelt for enkelte private rettssubjekter.

Norge mangler foreløpig en nasjonal CERT (Computer Emergency Response Team) som kan koordinere respons på IT-sikkerhetsangrep på nasjonalt nivå.

Sikkerhetstruende hendelser

NSM mottar rapporter om sikkerhetstruende hendelser. NSM kan imidlertid ikke utelukke at mange hendelser ikke rapporteres. Manglende rapportering vil gjøre det vanskeligere for NSM å få et reelt bilde av sikkerhetstilstanden.

4 Anbefalinger

Anbefalingene som gis under er et resultat av den vurderingen som er foretatt av risikobildet sett i sammenheng med sikkerhetstilstanden. Målet med anbefalingene er å styrke den defensive, forebyggende grunnsikringen i samfunnet i henhold til sikkerhetsloven. Grunnsikringen skal

redusere risiko for spionasje, sabotasje og terrorhandlinger. Rekkefølgen på anbefalingene under gjenspeiler ikke prioritet.

- Virksomhetenes praksis i forhold til verdivurdering må gjenspeile eventuelle endringer i risikobildet. NSM vil utarbeide en veiledning i verdivurdering.
- Det anbefales at virksomheter prioriterer gjennomgang og evaluering av egne sikkerhetstiltak.
- Det anbefales at virksomheter gjennomfører autorisasjonsprosessen i henhold til sikkerhetslovens bestemmelser.
- Virksomheter i en omstillingsprosess anbefales å ta spesielt hensyn til forebyggende sikkerhetstjeneste.
- Med bakgrunn i et endret risikobilde anbefales det at sektordepartementene fortsetter arbeidet med å fortløpende vurdere hvilke virksomheter som bør omfattes av sikkerhetsloven, i tillegg til de som i dag omfattes.
- NSM minner om virksomhetenes rapporteringsplikt i forhold til sikkerhetstruende hendelser og viser til NSMs veiledning i sikkerhetsadministrasjon: ”Reaksjon og rapportering ved sikkerhetstruende hendelser”. Veiledningen kan hentes på Internett: www.nsm.stat.no, under ”Regelverk”.