Nasjonal sikkerhetsmyndighet

NSMs Risikovurdering 2006

NSMs risikovurderinger er viktig for å gi overordnede myndigheter et bilde av utfordringer NSM, og virksomheter underlagt sikkerhetsloven, står overfor med tanke på den defensive forebyggingen mot terror, spionasje og sabotasje.

Risikovurderingene er også ment å gi virksomhetenes ledere og ansatte et bilde av de utfordringer som foreligger på sikkerhetssiden. Risikovurderingene skal bidra til at virksomhetene etablerer en bedre forståelse av hvorfor forebyggende sikkerhetstjeneste er viktig. I tillegg skal risikovurderingen legge et grunnlag for at virksomhetene forbedrer eget sikkerhetsarbeid der dette er nødvendig.

Forord

En gjennomtenkt forebyggende sikkerhetstjeneste er en første barriere i beskyttelsen mot terror og spionasje. Av den grunn er det viktig at vi alle er vårt ansvar bevisst med tanke på å skjerme ulike kategorier av informasjon og objekter. Alle ledere i virksomheter bør ha en tett dialog med egne ansatte for å finne frem til hvilken informasjon og objekter som har betydning for sikkerheten. En lignende dialog bør også skje på tvers av virksomheter. Det er summen av sikkerhetsarbeidet i de ulike virksomhetene som utgjør vår nasjonale sikkerhet.

Informasjonssikkerhet blir særlig aktuelt i en tid hvor PST vurderer etterretningstrusselen mot Norge og norske interesser til å være betydelig. En betydelig trussel er en alvorlig tilstand som bør spore oss alle til å holde en god kvalitet i vårt sikkerhetsarbeid.

Holdninger, motivasjon og forståelse er sentrale deler av en god sikkerhetskultur. Jeg vil anbefale alle ledere om også å fokusere på de kulturelle sidene av sikkerhetsarbeidet. Sikkerhetsarbeidet blir ikke bedre enn den rådende sikkerhetskulturen.

Vedtaket om å etablere et nasjonalt CERT hos NSM er et viktig tiltak. Kritisk infrastrukturs avhengighet av IKT-systemer gjør at Norge må skaffe seg virkemidler for å forebygge og håndtere digitale angrep. NorCERT vil bli en slags redningssentral som vil koordinere håndteringen av digitale angrep mot våre samfunnsviktige IKT-systemer.

Kjetil Storaas Hansen

Direktør

Nasjonal sikkerhetsmyndighet

NSMs Risikovurdering 2006

Forebyggende sikkerhetstjeneste i henhold til sikkerhetsloven skal gi samfunnet en grunnsikring mot sikkerhetstruende virksomheter som spionasje, sabotasje og terrorhandlinger. For å etablere en slik grunnsikring skal alle offentlige og private virksomheter underlagt sikkerhetsloven ha på plass et tilstrekkelig utvalg av forebyggende sikkerhetstiltak. Summen av egensikringen i den enkelte virksomhet utgjør en viktig del av samfunnets grunnsikring mot nettopp spionasje, sabotasje og terrorhandlinger.

NSMs risikovurderinger skal gi en fremstilling av sikkerhetssituasjonen innen de områder hvor NSM er engasjert. Risikovurderingene er viktig for å gi overordnede myndigheter et bilde av utfordringer NSM, og virksomheter underlagt sikkerhetsloven, står overfor med tanke på den defensive forebyggingen mot terror, spionasje og sabotasje. Med utfordringer menes her for eksempel utbedring av mangelfullt sikkerhetsarbeid, håndtering av kjente sårbarheter, identifisering av nye sårbarheter og å etablere gode interne sikkerhetsrutiner i den enkelte virksomhet.

I tillegg er risikovurderingene viktige for virksomheter underlagt sikkerhetsloven. Risikovurderingene er ment å gi virksomhetenes ledere og ansatte et bilde av de utfordringer som foreligger på sikkerhetssiden. Risikovurderingene skal bidra til at virksomhetene etablerer en bedre forståelse av hvorfor forebyggende sikkerhetstjeneste er viktig. I tillegg skal risikovurderingen legge et grunnlag for at virksomhetene forbedrer eget sikkerhetsarbeid der dette er nødvendig.

Denne ugraderte risikovurderingen fra NSM vil i hovedsak omhandle temaer og forhold knyttet til sikkerhetslovens krav til informasjonssikkerhet. Funn og erfaringer fra Varslingssystem for digital infrastruktur (VDI) beskrives ikke, det vises her til VDIs månedsrapporter på www.nsm.stat.no

NSM har gitt ut en gradert og en ugradert risikovurderinger fra 2003. For å få en større helhetlig forståelse av både risikobildet og sikkerhetstilstanden er det viktig å se årets vurdering i sammenheng med de foregående vurderingene. I de foregående vurderingene er det gått i dybden på ulike tema som ikke behandles i årets vurdering. De tidligere ugraderte vurderingene finnes på www.nsm.stat.no

Vurdering av trusselen

For at den enkelte virksomhet skal sikre seg selv mot trusselaktører er det viktig med kunnskap om hvem de skal beskytte seg mot. I tillegg er det viktig å ha kunnskap om hvilke metoder og teknikker de ulike trusselaktørene kan bruke for å ramme oss.

Politiets sikkerhetstjeneste (PST) vurderer etterretningstrusselen mot norske interesser som betydelig. En betydelig etterretningstrussel er en alvorlig tilstand som må spore til en målrettet innsats for å beskytte sikkerhetsgradert og annen sensitiv informasjon. NSMs erfaring er at flere virksomheter ikke i

tilstrekkelig grad tar hensyn til at etterretningstrusselen er betydelig. Sagt på en annen måte er flere offentlige virksomheter ikke bevisste nok i utøvelsen av egenbeskyttelse mot etterretningstrusselen.

Etterretningstrusselen eksisterer fremdeles i form av tradisjonell, statsinitiert spionasje. Terroraktører må også innhente informasjon for å kunne gjennomføre terrorhandlinger. Forsvar, industri, politiske beslutningsprosesser, internasjonalt samarbeid, krisehåndtering, ressursforvaltning, sårbare punkter i samfunn og teknologi er blant de mål som er attraktive i forhold til innhenting av informasjon ved bruk av fordekte midler (spionasje).

Summen av det sikkerhetsarbeidet som foregår i de respektive virksomhetene utgjør en viktig del av vår nasjonale sikkerhet. For NSM er det her vesentlig å få frem at det sikkerhetsarbeidet som skjer i den enkelte virksomhet også må ses i lys av den overordnede nasjonale sikkerheten.

I det påfølgende beskrives fem konkrete områder hvor sikkerhetsarbeidet i mange virksomheter har et forbedringspotensial. Til hvert av de beskrevne områdene vil det gis anbefalinger.

Verdivurdering

Hensikten med sikkerhetsarbeidet er at det finnes verdier som vi ønsker å skjerme. Det grunnleggende prinsippet er at sikkerhetsgradert informasjon skal beskyttes i hele sin livssyklus, fra informasjonen blir utarbeidet til den blir makulert eller avgradert. God informasjonssikkerhet kan beskrives som en viktig første barriere mot trusler som terror og spionasje.

En betydelig utfordring innen det forebyggende sikkerhetsarbeidet er at mange offentlige og private virksomheter ikke er flinke nok til å definere hvilken informasjon som er viktig å beskytte med utgangspunkt i det sikkerhetsloven beskriver som; rikets sikkerhet og selvstendighet og andre vitale nasjonale sikkerhetsinteresser. NSM har gjennom tilsyn og stikkprøver avdekket at flere virksomheter ikke er flinke nok til å verdivurdere informasjon, og derigjennom skille det sensitive fra det ikke sensitive.

Satt på spissen hjelper det lite at vi har omfattende sikkerhetsløsninger på IKT-siden, dersom vi ikke greier å identifisere hvilken innformasjon vi bør beskytte.

NSM anbefaler at alle virksomheter etablerer gode rutiner for å verdivurdere informasjon og objekter. NSMs *Veiledning i verdivurdering* anbefales lagt til grunn for de ulike sektorers utarbeidelse av interne rutiner for verdivurdering. Veiledningen er tilgjengelig på www.nsm.stat.no

På Internett finnes det i dag alle kategorier av informasjon, også informasjon som av sensitivitetshensyn ikke burde ha vært lagt ut på en hjemmeside eller sendt som e-post. Bakgrunn for dette kan være at utsteder av informasjonen ikke har verdivurdert informasjonen og følgelig ikke har erkjent at skjerming er nødvendig. Sensitiv informasjon kan være alt fra personsensitiv informasjon,

bedriftsensitiv informasjon eller informasjon som er av betydning for vår nasjonale sikkerhet. Internett gir videre gode muligheter for å sammenstille ikke sensitiv informasjon til et sensitivt bilde.

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. Samtidig, er det tilnærmet umulig å etterspore spredningen av utlagt informasjon, potensialet for spredning er i prinsippet uendelig, og informasjonen vil aldri med visshet kunne bli slettet.

NSM anbefaler at alle virksomheter etablerer gode interne rutiner for bruk av Internett for å hindre at sensitiv informasjon legges ut på nettet. Interne rutiner må ta hensyn til hvilke behov for beskyttelse som foreligger, herunder de lovmessige krav som måtte foreligge. I slike interne rutiner anbefales det fastsatt hvilken type informasjon som kan legges ut. Det er også en anbefaling at virksomhetens intern-kontrollrutiner inkluderer egen bruk av Internett. Et ytterligere poeng er at andre virksomheter bør varsles dersom disse skulle ha kommet i skade for å ha lagt ut sensitiv informasjon på nettet.

NSMs Temahefte 1/2005 *Internett og informasjonssikkerhet* beskriver denne problematikken i større grad. Temaheftet ligger på www.nsm.stat.no

Øvelser

Under øvelser trenes våre handlingsmønstre og planverk som er utarbeidet for å kunne komme best mulig ut av en krisesituasjon. Forhold som ikke tas tilstrekkelig hensyn til i forbindelse med øvelser, vil med stor sannsynlighet heller ikke fungere i en reell krisesituasjon.

NSM har dels gjennom deltagelse under øvelser, og dels gjennom besøk og tilsyn under øvelser, identifisert ulike sikkerhetsmessige forbedringspunkter for viktige nasjonale krisehåndteringsøvelser.

Her listes fire forhold hvor det etter NSMs syn foreligger et forbedringspotensial med tanke på vårt nasjonale øvelses- og krisehåndteringsarbeid:

- Under enkelte øvelser er ikke arbeidet med å skille sensitiv informasjon fra ikke sensitiv informasjon tilstrekkelig fokusert. En konsekvens av dette er i enkelte sammenhenger at informasjon som burde vært sikkerhetsgradert ikke blir det.
- Under øvelser deltar ofte personell som i det daglige ikke omgås sikkerhetsgradert informasjon. For at denne kategorien personell skal få tilgang til skjermingsverdig informasjon i forbindelse med øvelsen, kreves foruten en klarering, også en autorisasjon.[1] NSM har sett tilfeller der klarering og/eller autorisasjon mangler. Mangelfull bruk av taushetserklæringer ved tilgang til informasjon gradert BEGRENSET har også blitt registrert.

[1] Autorisasjon defineres i sikkerhetsloven som *avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående sikkerhetsklarering (med unntak for tilgang til informasjon sikkerhetsgradert BEGRENSET), bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov samt avlagt skriftlig taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad.*

- NSM har erfart at det foreligger ulike svakheter eller mangler med tanke på sikkerhetsgraderte informasjonssystemer.[2] Flere virksomheter har systemer som kan brukes internt i en virksomhet, men mangler ofte systemer for å kunne kommunisere med andre virksomheter. Resultatet av dette kan bli at informasjonsflyten under en reell krisehåndtering hemmes. Rask og målrettet informasjonsflyt er en suksessfaktor for å utøve en effektiv kriseledelse. Resultatet av mangler i evnen til å kommunisere på tvers, gjør det vanskelig å etablere et felles situasjonsbilde, hvilket er avgjørende under en krisehåndtering.
- Manglende utstyr til å kommunisere medfører i enkelte tilfeller at skjermingsverdig informasjon blir kommunisert over åpent eller ikke godkjent nett. NSM har her gjennom monitoring – slik det åpnes for i sikkerhetsloven – erfart at sikkerhetsgradert og annen sensitiv informasjon kommuniseres over ikke godkjente linjer. Informasjon omkring planverk, handlingsmønstre og personopplysninger har her vært kommunisert på en sikkerhetsmessig utilfredsstillende måte.
- De sikkerhetsmessige manglene som er listet ovenfor 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 enkelte øvelser. Evalueringsrapportene skal oppsummere hvilke forbedringspunkter som foreligger, og legge til rette for forbedringer under kommende øvelser.

NSM anbefaler at de sikkerhetsmessige sidene ved øvelser og krisehåndtering ivaretas på en tilfredsstillende måte. Dersom det skjer en forbedring omkring de forhold som her er listet vil det være et viktig steg i riktig retning.

Sikkerhetsadministrasjon

NSM har gjennom et eget prosjekt gått systematisk til verks for å kartlegge status for sikkerhetsadministrasjonen i sentrale deler av sivil forvaltning. Sikkerhetsadministrasjon er en samlebetegnelse på sikkerhetsorganisering, rapporteringsrutiner, instrukser, ansvarsforhold og metodiske krav til risikohåndtering. Metodene som ble benyttet i forbindelse med kartleggingen var en kombinasjon av spørreskjema og intervjuer. Funnene fra nevnte prosjekt supplerer de erfaringer NSM har gjort gjennom sin øvrige tilsynsaktivitet.

[2] Et informasjonssystem er gjennom sikkerhetsloven definert som *en organisert samling av periferiutrustning, programvare, kommunikasjonsnett som knytter dem sammen.* Et informasjonssystem kan være alt fra et større nettverk til PDAer, bærbare PCer og fotoapparater.

Kartleggingen synliggjør et bekymringsfullt avvik mellom foreliggende sikkerhetsadministrasjon og krav stilt i sikkerhetsloven og forskrift om sikkerhetsadministrasjon. Følgende funn illustrerer hvilke mangler som foreligger:

- flere virksomheter hadde ikke oversikt over sikkerhetsarbeidet i underlagte virksomheter
- flere virksomheter mottar ikke rapporter om sikkerhetsbrudd - eller andre sikkerhetstruende hendelser - fra underlagte virksomheter
- flere virksomheter har ikke rutiner for gjennomføring av sikkerhetsrevisjon
- flere virksomheter hadde ikke gjennomført sikkerhetsrevisjon
- flere virksomheter hadde ikke gjennomført kontroll med sikkerhetstilstanden i underlagte virksomheter

Andre funn som ble gjort i kartleggingen av sikkerhetsadministrasjon i offentlig forvaltning var at antall personell som helt eller delvis var tildelt sikkerhetsoppgaver, var for lavt. På enkelte områder var også den sikkerhetsfaglige kompetansen for lav. Et tredje funn er at flere virksomheter ikke etterlever kravene om å autorisere personell som skal få tilgang til gradert materiale.

Manglene tilknyttet sikkerhetsadministrasjon medfører at flere virksomhetsledere vanskelig kan etterkomme sitt sikkerhetsansvar. Uten en god sikkerhetsadministrasjon vil man verken kunne få oversikt over sikkerhetsarbeidet, kunne avdekke og utbedre mangler i sikkerhetsarbeidet eller kunne håndtere uønskede hendelser på en tilfredsstillende måte.

Det er således en klar anbefaling fra NSM at virksomhetsledere tar de nødvendige grep for å etablere sikkerhetsadministrasjon slik lovverket forventer det. Til hjelp i dette arbeidet anbefales NSMs Veiledning for sektordepartementene. Veiledningen finnes på www.nsm.stat.no

Informasjons- og kommunikasjonssikkerhet

God sikkerhet i våre datasystemer er avgjørende for å beskytte skjermingsverdig informasjon. IKT-sikkerhet er viktig fordi de store volumer av informasjon befinner seg nettopp i elektroniske lagringsmedia. NSM har gjennom sin tilsynsaktivitet avdekket at flere virksomheter ikke sørger for at egne IKT-systemer i tilstrekkelig grad er sikret. Mangelfull prioritering, ledelsesforståelse og kompetanse er her medvirkende årsaker. NSM finner dette bekymringsfullt.

Sett i lys av den foreliggende etterretningstrusselen skulle man kunne forvente at virksomhetene forsikret seg om at egne IKT-systemer er sikret i henhold til de forventninger lovverket stiller. Kravene som stilles i lovverket har til hensikt å forebygge at etterretningsaktører får tilgang til skjermingsverdig informasjon. Dersom IKT-systemene ikke er godt nok sikret vil skjermingsverdig informasjon eller objekter kunne bli eksponert for uautorisert personell, herunder etterretningsaktører.

En annen utfordring tilknyttet IKT-sikkerhet er bruk av små lagringsmedia som minnepinner. Det finnes dessverre eksempler på at gradert informasjon er hentet ut av graderte IKT-systemer via en minnepinne og i neste omgang sendt over Internett.

NSM anbefaler alle virksomheter om å være særlig bevisste på å sikre sine informasjonssystemer. NSMs veiledere innen området bør her legges til grunn. Relevante veiledere finnes på www.nsm.stat.no. I tillegg anbefales NSMs Temahefte 1/2006 Sårbarheter og trusler mot informasjonssystemer. I dette temaheftet gis det en beskrivelse av sentrale sårbarheter og trusler av betydning for sikkerheten i våre informasjonssystemer. Heftet ligger på www.nsm.stat.no.

NSM dekker videre to viktige funksjoner innen IKT-sikkerhet gjennom det nyetablerte NorCERT og SERTIT-ordningen. NorCERT skal bli et nasjonalt koordinerende organ for å håndtere alvorlige IKT-hendelser i internettilknyttede systemer av betydning for kritisk infrastruktur. SERTIT er en sertifiseringsordning for IT-produkter i henhold til internasjonale standarder. Bruk av sertifiserte produkter er et viktig bidrag for å oppnå en best mulig IKT-sikkerhet. Mer om SERTIT finnes på www.sertit.no

Sikkerhetskultur

Beskrivelsen av sikkerhetstilstanden i denne risikovurdering viser tilfeller av mangelfull sikkerhetskultur. Sentralt i begrepet sikkerhetskultur inngår begrepene holdning og motivasjon. Det er etter NSMs syn en sammenheng mellom manglende holdninger og motivasjon for å utøve en forsvarlig forebyggende sikkerhetstjeneste, og den på flere områder utilfredsstillende sikkerhetstilstanden i enkelte virksomheter.

Hvilke holdninger ledere legger for dagen er av særlig betydning for kvaliteten i virksomhetens sikkerhetsarbeid. NSM har gjennom sitt tilsyn sett at enkelte ledere i for liten grad fokuserer på sikkerhet. Medarbeideres holdning til sikkerhet er ofte en refleks av lederens holdning.

Målsetningene med sikkerhetsarbeidet kan vanskelig nås dersom motivasjon og holdninger svikter. Effekten av de ulike fysiske, personellmessige, IKT-relaterte og administrative tiltakene, som samlet skal beskytte informasjonen, vil bli redusert dersom ledelsen, de foresatte og den enkelte ansatte ikke sammen etablerer en god sikkerhetskultur. Sagt med andre ord vil effekten av de ressurser som settes inn for å beskytte informasjonen avta dersom forståelsen for, og viljen til å ta sikkerhetshensyn er mangelfull. Dersom ikke de kulturelle sidene av sikkerhetsarbeidet er tilfredsstillende betyr dette egeneksponering mot trusler som spionasje, sabotasje og i verste fall terrorhandlinger.

NSM ønsker et sterkere fokus på de kulturelle sidene av informasjonssikkerhetsarbeidet. For å sikre en vitenskapelig tilnærming samarbeider NSM med NTNU omkring sikkerhetskultur. Dette samarbeidet har resultert i rapportene *Informasjonssikkerhet og innsiderproblematikk (Kufås &*

Mølmann, 2003) og denne oppfølgeren; *Informasjonssikkerhet – atferd, holdninger og kultur (Nordby & Waale Hansen, 2005).* Rapportene finnes på www.nsm.stat.no

Foreløpige forskningsresultater fra NTNU tyder på at fokus på kulturelle forhold er viktig for å bedre forståelsen for, og kvaliteten i informasjonssikkerhetsarbeidet. De foreløpige funn tyder blant annet på at informasjonsmøter i små grupper, med aktiv deltakelse fra sluttbrukerne, er det mest effektive virkemidlet for å påvirke nettopp sluttbrukere.

Instrukser synes å ha liten effekt i forhold til kvaliteten i sikkerhetsarbeidet. Et annet foreløpig funn er at bedre synliggjøring av at den enkelte har et sikkerhetsansvar, noe som har sammenheng med integriteten som medlem av en organisasjon, gir positive effekter for sikkerhetsarbeidet. Et tredje foreløpig funn er at virksomheter må begynne å benytte andre tilleggsmidler enn tradisjonell kontroll, overvåkning og streng struktur i informasjonssikkerhetsarbeidet.

Som et konkret tiltak for å sikre økt fokus på sikkerhetskultur har NSM i samarbeid med NTNU og SINTEF utformet et verktøy som kan måle de kulturelle sidene av sikkerhetsarbeidet i en virksomhet. Med *SjekkIT-informasjonssikkerhet* tilbys et konkret verktøy som kan brukes til å måle en virksomhets sikkerhetskultur. Dels basert på slike målinger bør alle virksomheter utforme og gjennomføre tiltaksplaner for nettopp å bedre den interne sikkerhetskulturen. Verktøyet kan brukes av alle virksomheter, som av lovpålagte eller andre grunner skal beskytte sensitiv informasjon. Metodikken finnes på www.nsm.stat.no

Nasjonal sikkerhetsmyndighet (NSM)

NSM er et direktorat administrativt underlagt Forsvarsdepartementet, med faglig rapporterings- og ansvarslinje til Justis- og politidepartementet for saker i sivil sektor og til Forsvarsdepartementet for tilsvarende i militær sektor. NSM er nasjonal fag- og tilsynsmyndighet innen forebyggende sikkerhetstjeneste innen informasjons- og objektsikkerhet. Hensikten med sikkerhetsarbeidet er å gjøre samfunnet mer motstandsdyktig mot sabotasje, spionasje og terror. NSM dekker fagområdene IKT-sikkerhet, dokumentsikkerhet, personellsikkerhet, fysisk sikring, industrisikkerhet og sikkerhetsadministrasjon. I tillegg ligger SERTIT-ordningen og Varslingssentralen for digital infrastruktur og NorCERT inn under NSMs ansvarsområde.

NSMs samfunnsmål er å være en anerkjent og synlig pådriver for bedre sikkerhet i samfunnet.

Selve utøvelsen av forebyggende sikkerhetstjeneste er som hovedregel desentralisert idet alle virksomheter som håndterer sikkerhetsgradert informasjon og sikkerhetsklassifiserte objekter, skal utøve nettopp forebyggende sikkerhetstjeneste. Dette omfatter virksomheter både innen Forsvaret, øvrig statsforvaltning, fylkeskommunene, kommunene og leverandører som leverer varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser.

Nasjonal sikkerhetsmyndighet (NSM) Postboks 14 1306 Bærum postterminal Telefon: 67 86 40 00 Faks: 67 86 40 09 www.nsm.stat.no	Norwegian National Security Authority (NoNSA) P.O. Box 14 1306 Baerum postterminal Norway Telefon: + 47 67 86 40 00 Faks: + 47 67 86 40 09 www.nsm.stat.no