Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighets risikovurdering 2004, ugradert versjon

Innledning

Nasjonal sikkerhetsmyndighet (NSM) utarbeider årlig en risikovurdering. Hoveddokumentet er sikkerhetsgradert og distribueres til overordnede virksomheter som departementene og Forsvarsstaben. Dette dokumentet er en ugradert versjon av hoveddokumentet og tar for seg følgende punkter:

- NSMs oppgaver og rolle i samfunnet i forhold til andre instanser.
- NSMs metode for å utføre risikovurdering på nasjonalt nivå.
- Anbefalinger med bakgrunn i en vurdering av risikobildet sett i forhold til sikkerhetstilstanden i virksomheter.

NSMs oppgaver og rolle i samfunnet

NSMs oppgaver

NSM er administrativt underlagt Forsvarsdepartementet, men har også rapporteringslinjer til Justis- og politidepartementet. NSM er det utøvende organ i forhold til sikkerhetsloven[1] og er gitt oppgaver både som fagmyndighet og

[1] Lov av 20.mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

tilsynsmyndighet. NSM skal koordinere de forebyggende sikkerhetstiltakene for å avverge tilsiktede handlinger som spionasje, sabotasje og terror rettet mot informasjon og objekter av betydning for rikets sikkerhet og andre vitale, nasjonale sikkerhetsinteresser. NSM skal også kontrollere sikkerhetstilstanden. NSM innhenter og vurderer informasjon av betydning for gjennomføringen av forebyggende sikkerhetstjeneste, samarbeider internasjonalt, bidrar til at sikkerhetstiltak utvikles og gir informasjon, råd og veiledning. NSM er totalleverandør av kryptosikkerhetstjenester og godkjenner informasjonssystemer som skal behandle sikkerhetsgradert informasjon. NSM er klareringsmyndighet for øverste nivå og vedlikeholder det sentrale, nasjonale registeret over sikkerhetsklareringer.

NSMs forhold til andre aktører innen sikkerhets- og beredskapsarbeid

Den forebyggende sikkerhetstjenesten i henhold til sikkerhetsloven utøves i hovedsak i de enkelte virksomheter med NSM som koordinerende, kontrollerende og rådgivende nasjonalt organ. NSM yter dermed en slags ”hjelp til selvhjelp” overfor virksomhetene. Det er viktig å understreke at grensene mellom de instanser i samfunnet som utøver sikkerhets- og beredskapsarbeid på nasjonalt plan må være overlappende, grunnet kompleksiteten i samfunnet. Målet for alle parter bør være å skape et mest mulig motstandsdyktig samfunn overfor uønskede hendelser enten de kommer som et resultat av tilsiktede handlinger eller tilfeldige handlinger/hendelser.

Direktoratet for samfunnssikkerhet og beredskap (DSB)

Spionasje, sabotasje og terror manifesterer seg gjennom handlinger hvor det foreligger en intensjon om å samle inn informasjon ved hjelp av fordekte midler når det gjelder spionasje, og en intensjon om å skade når det gjelder terrorhandlinger og sabotasje. Grunnet intensjonen som foreligger ved disse handlingene, er det mulig å trekke et skille mot tilfeldige hendelser som naturkatastrofer, ulykker og menneskelig svikt, som også forårsaker skade. Slike hendelser skal i utgangspunktet forebygges og skadevirkninger begrenses av andre instanser i samfunnet enn NSM, og eksempelvis Direktoratet for samfunnssikkerhet og beredskap (DSB) vil her ha et overordnet, nasjonalt ansvar på vegne av Justis- og politidepartementet.

Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten

NSM koordinerer og utvikler forebyggende, defensive sikkerhetstiltak. Dette innebærer at NSM i hovedsak vil fokusere på sårbarhet og verdivurdering for å komme frem til de mest effektive, sårbarhetsreduserende tiltakene. Men det er grunn til å understreke at NSM har et kontinuerlig behov for informasjon om trusselaktører og deres intensjoner, kapasitet og fremgangsmåter. Slik informasjon er avgjørende for at NSM skal kunne utøve sin funksjon som koordinerende og kontrollerende organ innen forebyggende sikkerhetstjeneste. Informasjon om trusselaktører kommer blant annet fra PST og fra Etterretningstjenesten.

Andre instanser

Politiets spesialstyrker har en fremtredende rolle i bekjempelse av terroranslag og kan støttes av Forsvaret. Andre institusjoner enn de som alt er nevnt over

inngår også i samfunnets håndtering av sikkerhetstrusler som spionasje, sabotasje og terrorhandlinger. Foruten Regjeringen, påtalemyndigheten og domstolene kan en nevne Næringslivets sikkerhetsorganisasjon (NSO) og Næringslivets sikkerhetsråd (NSR).

NSM og VDI, SIS og SERTIT

Nedenfor gis en kort beskrivelse av NSMs tilknytning til Varslingssystem for digital infrastruktur (VDI), Senter for informasjonssikring (SIS) og Sertifiseringsordningen for IT-Sikkerhet (SERTIT).

Varslingssystem for digital infrastruktur (VDI)

Varslingssystem for digital infrastruktur (VDI) er etablert som en permanent ordning hos NSM. VDI er et partnerskap mellom etterretnings- og sikkerhetstjenestene. VDI er også et partnerskap mellom etterretnings- og sikkerhetstjenestene og ulike virksomheter (både private og offentlige) som samlet representerer samfunnskritisk infrastruktur og som har erfaring med beskyttelse av egne datanettverk. Deltagende virksomheter har installert sensorer på sine datanettverk som gjør det mulig å detektere ulike former for uønsket aktivitet fra internett mot virksomhetens digitale nettverk.

Senter for informasjonssikring (SIS)

NSM er med i styringsgruppen til prosjektet Senter for informasjonssikring (SIS) som er opprettet i Trondheim. SIS mottar hendelsesrapporter fra offentlige og private virksomheter og søker å kartlegge det totale trusselbildet mot norske IKT-systemer. SIS skiller seg fra VDI blant annet ved at VDI er et operativt system som i nær sanntid analyserer trusselen som dataangrep mot kritisk infrastruktur representerer, mens SIS ser på angrep mot IKT-systemer i en større sammenheng og på generell basis, basert på manuell innrapportering av hendelser fra berørte virksomheter.

SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet (SERTIT) er lagt til NSM. SERTIT forestår sertifisering av IT-produkter og systemer på bakgrunn av evalueringer gjennomført av godkjente evalueringsfirma (EVIT), som er en uhildet tredjepart. Hensikten med sertifiseringsordningen er å dekke myndighetenes og industriens behov for en kostnadseffektiv og rasjonell sikkerhetsmessig evaluering og sertifisering av IT-produkter og systemer. Dette skal bidra til å styrke tilliten til og bedre sikkerhetsnivået i IT-produkter og systemer. Ordningen er basert på Common Criteria (CC), som er en standardisert og internasjonal målestokk for IT-sikkerhet. Dette medfører at tilliten til produkter og systemer sertifisert etter CC lett kan sammenlignes med tilliten til andre produkter eller systemer sertifisert etter CC.

Andre viktige formål med ordningen er:

- Styrking av IT-sikkerheten i offentlig og privat sektor.
- Skape tillit til e-handelsløsninger og annen kommunikasjon nasjonalt og internasjonalt.
- Bidra til å gjøre norsk industri mer konkurransedyktig overfor utlandet.

Kontroll med NSM

Stortingets kontrollutvalg for etterretnings- og sikkerhetstjenestene: EOS-utvalget (www.eos-utvalget.no) gjennomfører jevnlig kontroll med NSM. Denne kontrollordningen er uavhengig av etterretnings- og sikkerhetstjenestene og forvaltningen for øvrig. Utvalgets medlemmer velges av Stortinget og utvalget rapporterer til Stortinget i form av årsmeldinger og særskilte meldinger.

Den løpende kontrollen utføres ved regelmessige inspeksjoner av tjenestene, både sentralt og i de enkelte virksomheter. Utvalget behandler klager fra enkeltpersoner og organisasjoner som mener tjenestene har begått urett mot dem.

Riksrevisjonen kontrollerer også arbeidet til NSM.

Risikovurdering på nasjonalt nivå

Security/Safety

Norske ord kan ha dobbel betydning. I sikkerhetssammenheng kommer dette til syne ved at både ”security” og ”safety” kan oversettes med ”sikkerhet” på norsk. Forskjellen mellom de to engelske begrepene er i hovedsak om de sikkerhetstruende hendelsene er forårsaket av tilsiktede handlinger som i ”security”, eller tilfeldige handlinger som i ”safety”.

Forebyggende sikkerhetstjeneste i henhold til sikkerhetsloven gjenspeiler det engelske begrepet ”security”. Trusselen består med andre ord i handlinger som er utført med viten og vilje av en spion, sabotør eller terrorist. Det er imidlertid grunn til å peke på de flytende overganger som eksisterer mellom ”security” og ”safety” for eksempel i forhold til handlinger som er et resultat av mangel på kunnskap, slurv og en generelt likegyldig holdning til sikkerhet. Slike handlinger har ikke nødvendigvis til hensikt å skaffe til veie skjermingsverdig informasjon for en som ikke har tilgang til denne (spionasje), eller forårsake tap som følge av skade på eiendom (sabotasje). Men konsekvensene av denne typen ubevisste handlinger kan være lik konsekvensene av tilsiktede handlinger utført av ondsinnede aktører. Forebyggende sikkerhetstjeneste har som mål å redusere *risikoen* for spionasje, sabotasje og terrorhandlinger.

Risikobegrepet

Begrepet ”risiko” kan ha ulikt innhold alt etter hvilken virksomhet som benytter begrepet. Det vil for eksempel være slik at oljesektoren utfører risikoanalyser rettet mot konkrete forhold, for eksempel ilandføring av gass fra en boreplattform. Analysen ser på sannsynligheten for at ulike hendelser skal inntreffe, og konsekvensen av slike hendelser. Hendelsene det her er snakk om vil gjerne være av tilfeldig karakter, og går dermed inn i ”safety” - terminologien. Det vil, ut fra en slik analyse, være mulig å sette opp en risikomatrise som gjør grad av risiko synlig ut fra beregninger. I et slikt tilfelle kan en operere med lav, middels og høy grad av risiko. NSM har så langt ikke funnet det hensiktsmessig å definere en generell grad av risiko på nasjonalt plan. NSM har imidlertid som mål å kunne si noe om hvilke sektorer som synes mer utsatt enn andre og på hvilke områder.

Risikobegrepet bygger på to komponenter; sannsynlighet og konsekvens. Det er ofte slik at *sannsynligheten* for at eksempelvis en terrorhandling skal begås er svært liten. Konsekvensene av handlingen kan imidlertid være så store at Stortinget har valgt å innføre et lovverk, sikkerhetsloven, som skal sørge for at en grunnsikring til enhver tid er på plass for informasjon og objekter av spesiell verdi for samfunnet gjennom å få på plass defensive sikkerhetstiltak.

Konsekvens har sammenheng med verdi på informasjon og objekter. Dess større verdi et objekt eller informasjon har, dess større blir konsekvensene dersom objektet blir ødelagt eller informasjonen blir kjent for uvedkommende. Det er derfor avgjørende at aktuelle virksomheter er i stand til å foreta en vurdering av hva som har sikkerhetsmessig verdi slik at objekter og informasjon som virkelig har betydning for rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser, blir beskyttet. Virksomhetene må være i stand til å se seg selv i en større, samfunnsmessig sammenheng ved verdivurderingen, samtidig som konsekvenser for egen virksomhet naturligvis også må tas hensyn til. Det er ikke mulig å beskytte absolutt alt, derfor må en gjøre et utvalg.

Sannsynligheten for at spionasje, sabotasje eller terrorhandlinger finner sted har blant annet sammenheng med egenskaper hos trusselaktøren. Stikkord her kan være **intensjon** og **kapasitet**. Det er verdt å merke seg at intensjonen, altså ønsket om for eksempel å utføre en terroraksjon, kan endre seg raskt. En årsak til at intensjonen endres kan være uventede hendelser som berører interesseområdet til terrorgrupperingen. Kapasiteten kan være konstant, men intensjonen kan altså endres hurtig.

Sannsynlighet henger også sammen med sårbarhet, altså egenskaper hos den som står i fare for å bli utsatt for spionasje, sabotasje eller terrorhandlinger. En kan gå ut fra at for eksempel et informasjonssystem som ikke har god nok beskyttelse i form av brannmurer vil være mer sårbart overfor angrep og at sannsynligheten for at dette informasjonssystemet rammes dermed vil være større.

Risikobildet

Begrepene sikkerhetsmessig verdi, sikkerhetstrussel og sårbarhet er komponenter i NSMs risikobilde.

Sikkerhetsmessig verdi

Utgangspunktet for all forebyggende sikkerhetstjeneste må være å kunne fastslå hva som trenger særlig beskyttelse. Formuleringen i sikkerhetsloven er at ”informasjon og objekter av betydning for rikets sikkerhet og selvstendighet og andre vitale nasjonale sikkerhetsinteresser” skal beskyttes og dermed har sikkerhetsmessig verdi. Det er ikke enkelt å fastslå hva som ligger i dette. For rikets sikkerhet synes det klart at *nasjonal handlefrihet og integritet* må være sentralt. Nasjonal handlefrihet og integritet kan brytes ned til underpunkter hvor følgende punkt kan være vesentlige:

- Konstitusjonell handlefrihet

- Økonomisk og finansiell handlefrihet
- Juridisk handlefrihet
- Militær handlefrihet
- Sikkerhetspolitisk handlefrihet
- Innenriks- og utenrikspolitisk handlefrihet
- Territoriell integritet

Oversikten er ikke uttømmende. Utfordringen for den enkelte virksomhet blir å definere hva som er kritiske verdier for sin egen del samtidig som virksomhetene ser seg selv i en større sammenheng.

For begrepet ”andre vitale nasjonale sikkerhetsinteresser” synes det nokså klart at nasjonale interesser knyttet til punktene under vil kunne komme inn under begrepet.

- Energi- og matforsyning
- Samferdsel og telekommunikasjon
- Helseberedskap
- Bank- og pengevesen
- Andre samfunnsøkonomiske forhold

Et sentralt spørsmål når det gjelder å vurdere om egen informasjon er skjermingsverdig 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 utgjør en så verdifull kunnskapsbase for mulige ondsinnede aktører at den helhetlige informasjonen vil kunne være skjermingsverdig i henhold til sikkerhetsloven.

Prinsippet om skjerming av informasjon for å gjøre sikkerhetstruende virksomhet så vanskelig som mulig kan bryte med et viktig prinsipp for å bekjempe spesielt terrorhandlinger, nemlig informasjonsdeling fra offentlige myndigheter og ut til befolkningen. Det er antagelig slik at ”mannen i gata”, gjennom sin årvåkenhet og evne til rapportering av mistenkelige personer/gjenstander/hendelser og lignende, stadig vil bli viktigere for å bekjempe terrorhandlinger i fremtiden. Dette innebærer at offentligheten har et informasjonsbehov. Verdivurdering må derfor også ta hensyn til om det faktisk kan være slik at en offentliggjøring av spesifikk informasjon knyttet til terrorhandlinger vil kunne være med på å forebygge terrorhandlingene i større grad enn en hemmeligholdelse av informasjonen.

Det kan være grunn til å spørre om ikke ”det informerte samfunn” også vil være ”det mest motstandsdyktige samfunn” i forhold til terrorhandlinger. Men balansegangen kan være hårfin, fordi det kan være tenkelig at visse typer informasjon som blir kjent for offentligheten vil kunne skape unødig redsel.

Sikkerhetstrusselen

Spionasjetrusselen eksisterer fremdeles i form av ulovlig etterretningsvirksomhet.
Mål for spionasjen[2] kan være følgende, uten at listen på noen måte er uttømmende:

- Norsk utenriks- og sikkerhetspolitikk
- Regjeringsbeslutninger
- Forsvaret
- Kritisk infrastruktur
- Industri, forskning og teknologi

Metoder for spionasjen kan være følgende, uten at listen på noen måte er uttømmende:

- Verving
- Observasjon
- Elektronisk utstyr
- IKT-systemer
- Ambassadepersonell

Sabotasje[3] innebærer en 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. Et eksempel på sabotasje kan være koordinerte angrep mot elektroniske informasjonssystemer som medfører tap av tilgjengelighet for informasjonen. Denne trusselen er reell i dag. Samfunnets avhengighet av datasystemer er stor og stadig økende. Dette gjør det stadig mer attraktivt å gjennomføre slike angrep, gjerne kalt DoS-angrep (Denial of Service).

Norge har så langt knapt nok vært utsatt for *terrorhandlinger*[4]. Det er derfor naturlig å se utenfor Norges grenser for å få et innblikk i eventuelle endringer i forhold til målutvelgelse og metoder.

Det internasjonale bildet er særlig preget av situasjonen i Midt-Østen. Her har bruk av selvmordsaksjonister blitt stadig vanligere. Åpent tilgjengelig statistikk viser at statlige mål er attraktive for terrorister. Typiske mål i denne kategorien er ambassader. Men det er verdt å legge merke til hvordan privatpersoner og privat eiendom ser ut til å bli stadig mer attraktive mål for terrorister. Statistikk indikerer at det har foregått en dreining bort fra statsrelaterte mål til statsborgere/private foretak og deres eiendom som mål. Dette kan være med på å illustrere terroristens valg av ”myke” mål, som privatpersoner og private

[2] Innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt, jfr. § 3 nr. 3 i sikkerhetsloven.
[3] Se § 3 nr. 4 i sikkerhetsloven.
[4] 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, jfr. § 3 nr. 5 i sikkerhetsloven.

virksomheter, fremfor ”harde” mål, som militære avdelinger og ambassader. Samtidig er det grunn til å bemerke at utviklingen i retning av stadig flere selvmordsbombere tilsier at også ”harde” mål kan bli utsatt for angrep.

Når det gjelder terroristers våpenbruk, så forteller statistikk at bruken av tradisjonelle eksplosiver, samt håndvåpen, dominerer stort i aksjonene.

Sårbarhet og mottiltak (utvalgte emner)

Den tredje og siste komponenten i risikobildet er sårbarhet. I det følgende vil det bli fokusert på noen forhold som kan ha betydning for sårbarhet, samtidig som enkelte tiltak for å redusere sårbarhet også angis.

Omstilling

Eierne stiller i dag store krav til lønnsomhet og effektivitet innenfor virksomhetene. Dette gjelder både statlig, kommunal og privat sektor. Forebyggende sikkerhetstjeneste synes å bli nedprioritert i forbindelse med omstilling som har til hensikt å bedre inntjening, eventuelt begrense utgifter.

Sentralisering er i mange tilfeller en viktig del av en omstillingsprosess. Sentralisering kan bidra til å samle kompetanse på ett sted, slik at denne kan komme virksomheten til nytte på en bedre måte enn tidligere, hvor kompetansen kanskje var fragmentarisk og spredt. Et sterkt, sentralisert fagmiljø kan også føre til at det blir attraktivt for nyutdannede å søke arbeid der, slik at man får en kontinuerlig utvikling av kunnskap.

Samtidig er det slik at en sentraliseringsprosess innebærer utfordringer for den forebyggende sikkerhetstjeneste. Et viktig punkt kan være at sikkerhetsadministrasjonen gjerne plasseres sentralt. Dermed mangler det lokale, underliggende ledd i en sikkerhetsorganisasjon. Konsekvensen av dette kan være at innenfor det lokale leddet mangler de ansatte forståelse for og innsikt i den forebyggende sikkerhetstjenesten. Dette kan øke sannsynligheten for kompromittering av informasjon.

Omstilling skal skje hurtig. Dette er ikke gunstig i forhold til dokumentsikkerhet. Ved omorganisering er det ofte problemer med å få full oversikt over hvor graderte dokumenter faktisk befinner seg. Det kan virke som om omstillingsprosessen gis meget høy prioritet slik at virksomheter blir gitt for liten tid til å få orden på arkiver, både fysisk og regnskapsmessig. Konsekvensen av dette er naturlig nok økt fare for kompromittering av informasjon.

Det er viktig å være oppmerksom på de nevnte forhold i en omstillingsprosess, slik at nødvendige forholdsregler kan tas. Det kan for eksempel være nødvendig å redusere hastigheten i en omstillingsprosess for å være sikker på at en har fullstendig kontroll.

Teknologisk utvikling

Teknologisk utvikling har betydning for sårbarhet. Teknologi kan gi nye muligheter som kan redusere sårbarhet, for eksempel gjennom avanserte brannmurer i et datasystem eller et avansert alarmanlegg som beskytter et skjermingsverdig objekt. Teknologi kan også føre til økt sårbarhet, noe som kan illustreres av følgende eksempel:

Sverige er i full gang med omstilling i forsvaret, i likhet med Norge. Den svenske forsvarsministeren har uttalt at få har kommet like langt som Sverige i

omstillingen mot et nettverksbasert forsvar. Det nettverksbaserte forsvaret er basert på bruk av avansert teknologi for å samordne informasjon i alle ledd i forsvaret slik at det til enhver tid skal være mulig å ha oversikt over situasjonsbildet.

> *I november 2002 ble tre personer arrestert i Sverige, mistenkt for spionasje rettet mot mobil- og telenettet. Alle var ansatte i Ericsson og arbeidet med forskning innen telekommunikasjon. I dag er en av de tre dømt til åtte års fengsel, en til fire år og den tredje er frikjent. Dommen på åtte år blir anket. Opplysninger tyder på at dersom spionasjen hadde vært vellykket, ville en fremmed statsmakt i verste fall ha blitt i stand til å manipulere det nettverksbaserte forsvaret i Sverige. Spionasjen var konkret innrettet mot å få tak i den teknikken som gjør det mulig å avlytte informasjon, altså konfidensialitetsrettede angrep, innvirke på informasjonen, altså integritetsrettede angrep eller rett og slett stanse informasjonsflyten (sabotasjeangrep).*

Fordi kommersiell teknologi i stor grad anvendes på tvers av landegrensene, blant annet grunnet krav til kostnader og kompatibilitet, kunne en vellykket spionasje rettet mot det svenske, fremtidige nettverksbaserte forsvaret kanskje ha gitt verdifull etterretningsinformasjon også i forhold til andre lands systemer. Bruk av såkalt hyllevare kan altså skape sårbarhet. Men dette er neppe en utvikling som det er mulig å reversere. Utfordringen ligger dermed blant annet i å skjerme hvordan en faktisk utnytter komponentene i et system og hvordan en kombinerer teknologien med operative handlinger.

Sårbarhet i forhold til avlytting

Avlytting av vanlige telefoner krever kun tilgang til spredenettet (de to trådene i veggen) til telefonsentralen. Normalt vil et spredenett gå til en egen hussentral plassert i bygningen, eller en kan ha linjer direkte fra en teleleverandør. Det er viktig å ha kontroll med hvor spredenettet går i bygningen. Normalt vil det ligge i vegg eller over himling i en etasje og i sjakt mellom etasjene til en fordelingsboks i kjelleren. Dersom en ikke har kontroll med denne ledningsføringen, kan telefonavlytting gjøres med enkle midler. Callinganlegg er også sårbare i forhold til avlytting.

Utbredelsen av mobiltelefoner er stor og stadig økende. En vanlig forestilling knyttet til bruk av mobiltelefon av GSM-typen er at samtalen krypteres og dermed er ”sikker”. Det er viktig å huske på at det kun er ”radiohoppet”, det vil si strekningen mellom mobiltelefonen og mobiltelefonmasten, som er kryptert.

Flere mobile GSM-systemer som simulerer å være basestasjon, det vil si at de opptrer som falske basestasjoner, er kommersielt tilgjengelige. GSM-telefoner kan avlyttes og dataoverføring monitoreres. GSM-telefonen tror den kommuniserer med basestasjonen når den i virkeligheten kommuniserer via den falske basestasjonen.

Det viktigste tiltaket mot kompromittering av informasjon ved bruk av mobiltelefon er rett og slett å være oppmerksom på muligheter som eksisterer for avlytting, og tilpasse ordbruken i samtalen deretter.

Fysisk sikring

Fysisk sikring av informasjon og objekter er en viktig del av de helhetlige, forebyggende sikkerhetstiltakene. De fysiske sikringstiltakene skal gi beskyttelse både mot spionasje, sabotasje og terrorhandlinger. En balansert, fysisk sikring oppnås ved at tiden en vinner ved de fysiske sikringstiltakene og tiden det tar før en oppdager anslaget, til sammen er mindre enn tiden det tar for en utrykningsstyrke å ta seg til stedet hvor anslaget finner sted. Evne til å reagere på en alarm med personell som rykker ut, er helt avgjørende for troverdigheten til sikkerhetstiltakene. Sagt med andre ord: Det hjelper ikke uansett hvor solide gjerder og avanserte alarmsystemer en virksomhet har dersom de ondsinnede aktørene vet at det ikke finnes personell som rykker ut ved alarm.

Eksplosiver og håndholdte våpen er de vanligste virkemidlene til terrorister. Det er vanskelig å beskytte bygninger mot eksplosiver. Hovedvirkningene av en eksplosjon er trykk og splinter. Bygninger med store glassflater vil være særlig utsatte. En av de fremste årsakene til personskader i bombeattentat, er kutt fra glass.

God avstand fra eksplosjonen er det mest effektive tiltaket for beskyttelse. I bystrøk er imidlertid dette tiltaket i de fleste tilfeller ikke gjennomførbart. Bygningskropp og vinduer kan også forsterkes. En forsterkning av bygningskroppen er imidlertid svært vanskelig å utføre i etterkant. Vakthold og sikring, kontroll med personell og vareleveranser samt innhenting av trusselinformasjon fra offentlige myndigheter, er ofte de tiltakene som er mest realistisk å gjennomføre for de enkelte virksomheter.

Sårbarhet i informasjonssystemer

Truslene mot dagens informasjonssystemer er mange og varierte. Sårbarheter må reduseres for å begrense mulighetene for trusselaktører til å gjennomføre angrep. NSM fokuserer først og fremst på sårbarhetsreduserende tiltak som skal redusere risiko for at sikkerhetsgradert informasjon kompromitteres eller på andre måter mister sin verdi. Mange av prinsippene for sikring av denne type informasjon vil naturligvis kunne være til stor hjelp for å sikre alle former for sensitiv informasjon, selv om informasjonen faller utenfor sikkerhetslovens virkeområde.

”Sårbarheten til et system er et uttrykk for de svakheter og mangler som finnes i systemet og spesielle omstendigheter som øker sannsynligheten for at trusler vil materialisere seg i en sikkerhetshendelse. Eksempler på spesielle omstendigheter kan være størrelse, kompleksitet, at mange aktører er involvert, geografisk spredning, hyppige endringer og utsatt beliggenhet.”[5]

[5] *”Nasjonal strategi for informasjonssikkerhet - utfordringer, prioriteringer og tiltak”*, utgitt av Nærings- og handelsdepartementet juni 2003 (www.enorge.org).

Siden antall informasjonssystemer som kobles sammen øker, vil det her fokuseres på sårbarheter i store informasjonssystemer. Store informasjonssystemer blir mer komplekse da de består av flere komponenter, tilbyr et høyere antall tjenester og tjener mange brukere.

Dersom man betrakter en stor, distribuert infrastruktur, er det flere faktorer som må vurderes nøye ut fra et sikkerhetsmessig ståsted. Under presenteres faktorer som kan være opphav til sårbarheter i informasjonssystemer

Menneskelige feil: Det er mange risikokilder forbundet med informasjonssystemer. Blant de største er menneskelige feil, både tilsiktede og utilsiktede. Et eksempel på en typisk menneskelig feil er valg av enkle passord som lett lar seg gjette.

Mye informasjon: Et stort informasjonssystem inneholder mye informasjon som brukerne har teoretisk tilgang til. Autoriserte brukere kan få tilgang til mer informasjon enn det de har behov for (”need-to-know”).

Store konsekvenser: Angrep på store systemer vil være mer attraktivt å utføre, da et enkelt angrep vil kunne ramme store deler av nettverket. Stor informasjonsmengde gjør informasjonssystemene mer interessante for spionasje og sabotasje. Informasjon om ulike terrorgrupperinger tyder også på at faren for terrorangrep mot store informasjonssystemer ikke skal undervurderes, til tross for at en hittil ikke har sett de store anslagene. Det er sannsynlig at et stort informasjonssystem vil være et mer attraktivt mål for angrep enn et mindre system.

Flere komponenter: Store informasjonssystemer består av mange komponenter som alle må fungere sammen og sikres. Et økende antall komponenter fører til mer kompleks konfigurasjon, integrasjon og administrasjon. Mange komponenter vil også øke kompleksiteten i forbindelse med drift og vedlikehold.

Større angrepsflate: Store informasjonssystemer tilbyr flere tjenester. Dermed er det også flere veier inn til systemene. Det er viktig at alle disse veiene sikres på en tilfredsstillende måte. For eksempel fører hjemmekontorløsninger via Virtuelle Private Nettverk (VPN) til et økt antall klienter. De nye klientene utvider nettverket og gir en inngangsmulighet til informasjonssystemet på arbeidsplassen som kan utnyttes av ikke-autoriserte brukere.

Rasjonalisering av teknisk personell: I et stort informasjonssystem vil det kreves kompetanse innen en mengde ulike fagfelt både for utvikling og operativ anvendelse av veiledninger. Manglende kompetanse og nedbemanning blant personell fører til svekket sikkerhet i systemene.

Integrasjon av systemer og produkter: I store informasjonssystemer integreres nye produkter med de eksisterende. En har varierende kontroll med de nye produktene når det gjelder muligheter for skjulte feil og mangler. Dagens produkter har høy grad av funksjonalitet og er lett tilgjengelige, men mangel på teknisk kompetanse gjør det til en utfordring å integrere dem i allerede eksisterende systemer.

Mobile enheter: En annen teknisk sikkerhetsrisiko er den økende bruken av mobile enheter. Disse skaper sårbarheter i form av økt distribusjon av store

mengder informasjon utenfor virksomhetenes kontrollerbare områder. Lagring av informasjon på små, portable enheter medfører en økt risiko for at gradert informasjon kan komme på avveie, enten ved at enhetene mistes eller at de blir stjålet.

Tiltak for å redusere sårbarhet i informasjonssystemer

Alt sikkerhetsarbeid krever kontinuitet og en evne til helhetlig tankegang. NSM har til nå hatt sitt hovedfokus på forebygging. Særlig i forhold til informasjonssystemer er det imidlertid grunn til å peke på at NSM også er engasjert i deteksjonstiltak og reaksjonstiltak gjennom VDI. Det vurderes om det skal etableres et nasjonalt Computer Emergency Response Team (CERT). Dette vil i tilfelle ha en rolle i forhold til gjenoppretting av informasjonssystemer, idet en nasjonal CERT er tenkt å skulle bidra med råd, veiledning og koordinering ved større, koordinerte dataangrep. VDI ser i dag stadig forsøk på kartlegging av datasystemer tilhørende kritisk infrastruktur, for å finne sårbarheter. Sårbarheter kan blant annet utnyttes i forbindelse med innbrudd, tjenestenekt (Denial of Service)[6] og planting av ormer[7].

NSM utgir **veiledninger** innen en rekke fagfelt. Bruk av veiledningene vil gi et sikrere system. I tillegg til de overordnede veiledningene, utvikler NSM produktspesifikke implementasjonsveiledninger. Veiledningene finnes på NSMs hjemmeside: www.nsm.stat.no.

En viktig del av NSMs forebyggende sikkerhetsarbeid består av å teste ulike løsninger. Formålet med dette er å få kjennskap til hvor god sikkerheten i nye teknologier og produkter faktisk er. **Forskningsarbeidet** er et viktig grunnlag for å kunne skrive generelle og produktspesifikke veiledninger.

NSM har i mange år **utviklet** og bidratt i industriens utvikling av kryptoutstyr med en sikker implementasjon av kryptoalgoritmer i hardware. En ny trend de siste årene har vært utviklingen av mobilt, enbruker kryptoutstyr. Et eksempel er NSK 200, en GSM mobiltelefon for sikker overføring av tale og datakommunikasjon. Andre eksempler er VPN[8]-utstyr som muliggjør sikker fjernaksess gjennom usikker infrastruktur (for eksempel internett eller en telefonlinje) inn mot informasjonssystemet, samt sikring av data lagret på en eventuell bærbar PC.

Sikkerhetstilstanden

Kjennskap til alle faktorene i risikobildet er en forutsetning for å være i stand til å innrette forebyggende sikkerhetstiltak på en hensiktsmessig måte. Risikovurderingen skjer ved å sammenholde kunnskap om risikobildet og kunnskap om sikkerhetstilstanden.

---

[6] En server kan for eksempel bli ”bombardert” med elektronisk post slik at den slutter å fungere.
[7] ”Ormer” skiller seg fra ”virus” ved at ormer spres uten brukermedvirkning. Det er med andre ord ikke nødvendig eksempelvis å åpne et vedlegg til en e-post for at maskinen skal bli infisert.
[8] ”Virtuelle private nettverk”.

Informasjon om sikkerhetstilstanden innhentes på flere måter: NSMs tilsyn[9] er en viktig måte å få kunnskap om hvordan tilstanden er. En annen måte som gir kunnskap om sikkerhetstilstanden, er å utnytte virksomhetenes rapportering av sikkerhetstruende hendelser[10] for å danne seg et bilde. En tredje måte som kan gi informasjon om sikkerhetstilstanden, er å følge med på oppslag i media som indikerer at tilstanden kan være dårlig innenfor et bestemt område.

Begrepet "sikkerhetstilstand" inneholder blant annet følgende momenter:

1) Hvordan vurderer virksomhetene hvilken sikkerhetsgradering den informasjonen som utarbeides skal få?
2) Er sikkerhetsloven med forskrifter fullt ut implementert i virksomhetene?
3) Er regelverket egnet til å ivareta samfunnets behov for grunnsikring mot spionasje, sabotasje og terrorhandlinger?

Svar på disse tre spørsmålene samt rapportering/oppslag i media, sammenholdt med informasjon om risikobildet, gir grunnlag for anbefalinger. Anbefalingene skal blant annet peke på skjevheter knyttet til innretningen av sikkerhetstiltakene og virksomhetenes prioriteringer innen forebyggende sikkerhetstjeneste, samt påpeke mangler ved regelverket. Kanskje er det slik at enkelte områder prioriteres for lite og andre områder for mye innen forebyggende sikkerhetstjeneste? Begge deler er lite gunstig for grunnsikringen i samfunnet og kan føre til økt risiko for å bli rammet av spionasje, sabotasje eller terrorhandlinger.

[9] NSM utøver tilsyn for å kontrollere og gi råd/veiledning innen blant annet sikkerhetsadministrasjon, personellsikkerhet, administrativ krypto, informasjonssystemsikkerhet, industrisikkerhet, elektromagnetisk stråling (TEMPEST), tekniske sikkerhetsundersøkelser (TSU) og fysisk sikring.
[10] Se § 1-2, nr. 2 i Forskrift om sikkerhetsadministrasjon av 29. juni 2001 nr. 723.

Anbefalinger

- Det er viktig å understreke at selv om fokus innen forebyggende sikkerhetstjeneste i dag i stor grad rettes mot å avverge terrorhandlinger, så er det ingen grunn til å undervurdere etterretningstrusselen i form av spionasje. Teknologisk utvikling gjør at metodene som benyttes i forbindelse med spionasje blir stadig mer avansert. Det er derfor av vesentlig betydning at adgangskontroll og fysiske sikringstiltak prioriteres tilstrekkelig, slik at for eksempel utplassering av elektronisk utstyr for avlytting blir gjort så vanskelig som mulig.

- Mange prosjekt, for eksempel oppføring av store, vitale bygninger og installering av store informasjonssystemer, tar ikke hensyn til forebyggende sikkerhet før det har gått alt for lang tid. Det er derfor en utfordring å få på plass et system som bringer forebyggende sikkerhet inn på et tidlig stadium. Det er nettopp det å være i forkant som skal kjennetegne forebyggende sikkerhet.

- Det er behov for at det skjer en holdningsendring, spesielt blant brukerne av store, elektroniske informasjonssystemer, slik at sikkerhet blir tatt på alvor. Samfunnet taper hvert år store beløp på at informasjonssystemer ikke er operative. Manglende evne til å operere kan være forårsaket av en lite bevisst holdning til sikkerhet.

- Det er viktig at sikkerhetsarbeidet pågår kontinuerlig, slik at det bygges en kultur i virksomheten hvor sikkerhet tas på alvor. Lederen for virksomheten må ta sitt pålagte ansvar for sikkerhet etter sikkerhetsloven alvorlig, samtidig som de enkelte ansatte må være klar over at de utgjør leddene i kjettingen som totalt sett bestemmer om sikkerhetsnivået i virksomheten er godt.