Nasjonal sikkerhetsmyndighet

Rapport om sikkerhetstilstanden 2011

Juni 2012

Innhold

1 Forord

Rapport om sikkerhetstilstanden gir Nasjonal sikkerhetsmyndighet (NSM) sin vurdering av hvordan spesifikke mangler og svakheter ved det forebyggende sikkerhetsarbeidet og sikkerhetstilstanden generelt kan bidra til at trusselaktører realiserer sine mål gjennom å utnytte sårbarheter. Rammen for rapporten er sikkerhetsloven med forskrifter og andre forhold utenfor sikkerhetslovens område som anses relevant, særlig innenfor NSMs arbeidsområde i forhold til internettsikkerhet

NSM begrenser seg primært til vurderinger knyttet til sikringen av *informasjon* som er av betydning for Norges eller alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser. Forskrift om objektsikkerhet trådte i kraft 1. januar 2011. Virksomhetene er i ferd med å implementere forskriften. Da rapporten ble skrevet var ingen objekter meldt inn til NSM.

Den gir en vurdering av tilstanden innen forebyggende sikkerhet basert på tilgjengelig empiri fra:

- NSMs tilsynsvirksomhet iht. sikkerhetsloven.
- Innrapporterte og observerte sikkerhetstruende hendelser og sikkerhetsbrudd iht. sikkerhetsloven.
- Rapporter i forbindelse med NSMs arbeid med industrisikkerhet.
- NSMs avdeling NorCERT sin oversikt over hendelser på Internett og analyse og håndtering av dem.
- Tekniske sikkerhetsundersøkelser av rom og bygninger.
- Fagkunnskap om system- og nettverkstekniske aspekter relatert til sikkerhet, som blant annet inntrengingstester og emisjonssikkerhetstester.
- Personkontroll og personellsikkerhet.
- Øvelser.
- Fagkunnskap om kryptologi og kryptosikkerhet.
- Andre sikkerhetsmessige forhold av interesse for sikkerhetstilstanden.

Rapporten bør ses i sammenheng med vurderinger fra Politiets sikkerhetstjeneste (PST), Etterretningstjenesten (E-tjenesten), Forsvarets sikkerhetsavdeling (FSA), NATOs Allied Command Counterintelligence Jåtta Detachment, Kripos og Næringslivets sikkerhetsråd (NSR).

Det foregår flere prosesser som påvirker det forebyggende sikkerhetsarbeidet i Norge, blant annet:

- Ny langtidsplan for Forsvaret, med eget kapittel om cybersikkerhet
- Ny Stortingsmelding om samfunnssikkerhet
- 22. juli-kommisjonens konklusjoner og anbefalinger
- Evaluering av sikkerhetsloven
- Nye nasjonale retningslinjer for informasjonssikkerhet, hvor NSMs forslag til nasjonal cyberstrategi skal tas inn
- Implementering av objektsikkerhetsregelverket
- Forsvarssektorens retningslinjer for informasjonssikkerhet
- Nytt etterretningsdirektiv og ny etterretningsdoktrine.

Disse prosessene vil kunne få betydning for sikkerhetstilstanden i fremtiden. Prosessene bør sees i sammenheng og vurderes i forhold til gjeldende tilstand på det forebyggende så vel som operative sikkerhetsarbeidet i Norge og hos allierte.

2 Sikkerhetstilstanden

Sikkerhetstilstanden blir fortsatt svekket i Norge. Risikoforståelsen knyttet til spionasje, sabotasje og terror er fortsatt for lav, og viktige tiltak som risikovurderinger, kompetanseheving, rapportering og sikkerhetsrevisjoner blir ikke gjennomført.

Det er vesentlige mangler og svakheter i det forebyggende sikkerhetsarbeidet. Arbeidet og tiltakene som utvikles og iverksettes på dette området er mange og økende. Samtidig øker truslene i et mye raskere tempo. Dette medfører en situasjon med økende sikkerhetsmessig risiko, som får negative konsekvenser for sikkerhetstilstanden. Den grunnleggende hovedutfordringen er at den generelle risikoforståelsen på alle samfunnsnivåer er på et utilfredsstillende nivå.

NSM vurderer at vi har fått en situasjon med økende sikkerhetsmessig *risiko*. Det er vesentlige mangler i det forebyggende sikkerhetsarbeidet med konsekvenser for den nasjonale sikkerhetstilstanden. Dette representerer en sårbarhetsutfordring, da manglene kan utnyttes av trusselaktører med stadig økende kapabiliteter og kapasiteter.

- Det er generelt slik at de *verdier* vi ønsker å beskytte øker i volum og betydning i takt med samfunnsutviklingen og den økende produksjonen av informasjon.
- *Truslene* mot sikkerhetsgradert og annen skjermingsverdig informasjon er i sterk økning; særlig at den teknologiske oppfinnsomheten med hensyn til utvikling av skadevare på IKT-systemer akselererer. Trusselaktørene blir både mer selektive i sine mål og mer avanserte i sine metoder.
- *Sårbarheter* som kan utnyttes oppdages stadig, og dette øker mulighetene for at uvedkommende får tilgang til skjermingsverdig informasjon.
- *Tiltak* for å redusere sårbarheter utvikles ikke i samme takt som truslene og er i utgangspunktet utilstrekkelige.

Store sikkerhetsutfordringer

NSM har registrert alvorlige sårbarheter hos virksomheter som leverer samfunnskritiske tjenester. Disse sårbarhetene kan bli, og har blitt, avdekket og utnyttet på en måte som kan få store sikkerhetspolitiske og/eller økonomiske konsekvenser. NSM er bekymret for utviklingen når det gjelder grunnleggende kryptoinfrastruktur. Fortsetter utviklingen, er det også risiko for at høygradert skjermingsverdig informasjon, spesielt i forsvarssektoren, blir kompromittert og dermed utsatt for utnyttelse av ondsinnede trusselaktører som fremmed etterretning. I tillegg eksisterer det store sikkerhetsutfordringer rundt sikkerhetsklarering av personer og virksomheter, og manglende rapportering om egen sikkerhetstilstand.

Mange virksomheter underlagt sikkerhetsloven mangler gode styringssystemer for forebyggende sikkerhet. Dette kan føre til sikkerhetsorganisasjoner som ikke er dimensjonert for risikoen de skal håndtere og at ledelsen ikke setter av tilstrekkelig ressurser og kompetanse til arbeidet. Ofte er heller ikke virksomhetenes styringssystem for forebyggende sikkerhet koordinert med andre styringssystemer.

Menneskelige faktorer, som grunnleggende risikoforståelse, kunnskap, kompetanse, vilje, forståelse og holdninger må være på plass for at organisatoriske og tekniske aspekter ved sikkerhetsarbeid skal

fungere etter sine intensjoner. Med dårlig risikoforståelse blir kvaliteten på det forebyggende sikkerhetsarbeidet utilfredsstillende. Virksomheter mangler ofte nødvendig oversikt over hvilke verdier de besitter og eventuelt må beskytte. Truslene mot en rekke samfunnsverdier – som sensitiv og skjermingsverdig informasjon og samfunnskritiske objekter og funksjoner – er under kontinuerlig utvikling. Trusselaktører, med stadig økende resurser og kapasiteter, har en rekke metoder og virkemidler de kan ta i bruk for å utnytte sårbarheter og realisere sine mål. Dette ble bekreftet gjennom avdekkelse av flere alvorlige spionasjeforsøk i 2011.

Vi lever i et nettverkssamfunn, hvor to eller flere samfunnsfunksjoner ofte er avhengige av hverandre. Et angrep på, eller skader ved en enkelt funksjon eller et objekt kan derfor få konsekvenser som rekker langt utover skadene eller tapet på den direkte rammede samfunnsfunksjonen.

Alvorlige svakheter

Viktige IKT-systemer blir ofte ikke tilstrekkelig beskyttet og sikret. Konsekvensen kan blant annet være at spionasjeoperasjoner med potensielt store konsekvenser kan gjennomføres i Norge uten å bli oppdaget. Gjennom inntrengingstesting i både sivil og militær sektor har NSM påvist svært alvorlige svakheter. Svakhetene kan gi tilgang til både å manipulere, endre og slette både svært sensitiv informasjon og høyt sikkerhetsgradert informasjon. Testene viser at det koster lite å bryte seg inn i mange kritiske datasystemer. Dette er svakheter som har kunnet gi en trusselaktør tilgang til, og mulighet til å manipulere, endre og slette, både svært sensitiv informasjon og høyt gradert informasjon.

Et økende gap

NSM har tidligere rapportert om et økende gap mellom trussel og sikkerhetstiltak. Trenden er at dette gapet fremdeles øker. Ettersom risikoen mot skjermingsverdig informasjon, kritisk infrastruktur og samfunnsviktige funksjoner er stadig økende, kan det konkluderes med at 2011 var et år hvor sikkerhetstilstanden i Norge fortsatt ble svekket.

I tiden fremover er det god grunn til å holde øye med følgende trender:

- En fortsatt økning i alvorlige IKT-hendelser
- Mer profesjonell utvikling av ondsinnet programvare
- Målrettede angrep mot lukkede nett.
- Forsøk på å infiltrere prosesskontrollsystemer
- Spredning av skadevare over mobile enheter
- Misbruk av og infisering av smartkort og smartkortlesere
- Sårbarheter i leverandørkjeden av IKT-utstyr.
- Økt forespørsel etter klarering av personell med tilknytning til andre stater

Selv robuste IKT-systemer vil ikke være fullt sikret mot ukjente tekniske trusler og de avanserte aktivitetene som utgjør de alvorligste utfordringene mot rikets sikkerhet og vitale nasjonale sikkerhetsinteresser. For å redusere det økende gapet mellom sikkerhetstilstanden og trusselbildet, er det nødvendig å styrke robustheten i kritiske IKT-systemer, vår etterretningsevne, etterforskningsevne, og vår evne til å oppdage og håndtere alvorlige IKT-hendelser.

3 Risikobildet

Risikobildet er dynamisk. Risikobildet er sammensatt av en vurdering av **verdier** som må beskyttes, **trusselbildet**, samt hvilke **sårbarheter** som kan utnyttes for å ramme verdiene.

En grunnleggende forutsetning for forebyggende sikkerhet er at den eller de som er ansvarlige for sikkerheten har et så rettidig og korrekt risikobilde som mulig, gjennom jevnlige risikovurderinger. Det kan ikke gjennomføres balanserte og målrettede forebyggende sikkerhetstiltak uten en god risikoforståelse. For informasjon og objekter som skal beskyttes med hjemmel i sikkerhetsloven er kravene til beskyttelsestiltak i sikkerhetsloven å anse som minimumstiltak. Når sikkerhetstilstanden evalueres, skal ytterligere tiltak utover minimumskravene vurderes gjennomført. For verdier som skal beskyttes med hjemmel i sikkerhetsloven, må må det legges til grunn at trusselaktørene antas å ha betydelige ressurser og høy kapasitet.

Dersom sikkerhetsgradert informasjon blir gjort kjent for uvedkommende, kan dette få skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser.

Det vil særlig være viktig å beskytte informasjon eller objekter som støtter:

- Sikkerhetspolitisk krisehåndtering og forsvar av riket, herunder
  - Beredskapsplaner; militære og sivile
  - Informasjon om Forsvarets operative evne (materiell, infrastruktur, objekter, kapasiteter etc.)
  - Kommando-, kontroll- og informasjonssystemer
- Kritiske infrastrukturer, særlig
  - Kraft
  - Telekommunikasjon
  - Finans
- Økonomisk aktivitet av nasjonal betydning, for eksempel med hensyn til beskyttelse av kritisk informasjon om:
  - Olje- og gassindustrien
  - Maritim industri
  - Finans- og bankvesen
  - Forsvarsindustri
- Beskyttelse av befolkningens liv og helse, i forhold til for eksempel
  - Bekjempelse av terrorisme og annen alvorlig kriminalitet
  - Håndteringsevne i forhold til pandemisk sykdom.

Samfunnets avhengighet av IKT og Internett har blitt en strategisk sikkerhetsutfordring. Både myndigheter og private virksomheter er avhengig av disse for å levere tjenester. Sikkerhetsutfordringer retter seg mot alle nivåer i samfunnet, fra beskyttelse av enkeltpersoners pc-er og mobiltelefoner, til beskyttelse av systemer og objekter som er avgjørende for samfunnskritiske funksjoner.

Cybersikkerhet har for mange av Norges allierte hatt høy prioritet de siste årene. Det er stort skadepotensiale ved cyberangrep mot samfunnskritiske tjenester og kritisk infrastruktur.

Norge er et nettverkssamfunn med stor, og ofte gjensidig avhengighet mellom samfunnskritiske funksjoner. Denne avhengigheten går på tvers av sivil-militære og offentlig-private skiller og også over landegrenser. Det er stor grad av elektronisk samhandling, og verdi av mengden informasjonen som utveksles øker.

Det er tett avhengighet mellom IKT-infrastruktur og strømforsyning. Sikker tilgang på strøm og energi er særlig kritisk for tilbydere av IKT og for virksomheter som er avhengig av IKT. Denne avhengigheten representerer en vesentlig sårbarhet i samfunnet.

Samfunnet har blitt mer sårbart for selv korte driftsavbrudd i systemer og nett. Den økte sårbarheten skyldes blant annet økt teknisk kompleksitet og tettere sammenkobling.

Økende produksjon av sensitiv informasjon og digitaliseringen av samfunnet tilsier at økende mengder sensitiv og kritisk informasjon plasseres i Internetteksponerte fysiske lagringsenheter og IKT-systemer. Store mengder sensitiv informasjon er blant annet tilgjengelig via åpne kilder og andre ugraderte informasjonssystemer på Internett. Dette gjelder både informasjon fra offentlig forvaltning, industri og næringsliv. Dette er informasjon som kan være viktig for beskyttelse av vitale nasjonale interesser og verdier, som liv og helse, et godt miljø, den nasjonale økonomien, samfunnskritiske funksjoner, krisestyring i fred, krise og krig, det politiske systemets troverdighet, samt rikets sikkerhet og selvstendighet og vitale nasjonale sikkerhetsinteresser.

Mange offentlige og private samfunnskritiske tjenester har satt bort drift av sine servere og databaser i private datasentre. Flere av disse datasentrene lagrer eller vil komme til å lagre data av betydning for rikets sikkerhet og vitale nasjonale sikkerhetsinteresser. Flere store datasentre er under utvikling og prosjektering.

I tillegg vil flere samfunnskritiske virksomheter etterhvert lagre data i nettskyen.

Verdien av samfunnets sensitive og skjermingsverdige informasjon øker, både i sivil og militær sektor.

Etterretningsaktiviteten mot Norge og norske interesser vurderes av PST å være vedvarende høy, og etterretning ved hjelp av IKT og Internett øker. Det er avdekket flere tilfeller av etterretningsoperasjoner mot norske myndigheter og bedrifter i 2011. Det pågår stadig etterretningsoperasjoner ved bruk av ondsinnet programvare.

Fremmede staters etterretningstjenester søker primært å innhente informasjon som kan fremme landets politiske og økonomiske interesser. Aktiviteten er hovedsakelig rettet mot forsvars- og sikkerhetspolitikk, olje- og gassektoren, høyteknologi-/ forsknings-/undervisningsmiljøer og eksilmiljøer. Tradisjonell militær etterretning mot militære kapasiteter fortsetter.

Trusselen mot private leverandører av sikkerhetsgraderte anskaffelser vil i en del sammenhenger være høyere enn trusselen mot forvaltningsorganer, da informasjonen også kan ha verdi som forretningshemmeligheter som det kan gi stor økonomisk fordel å få tilgang til. Risikoen for at virksomheter underlagt sikkerhetsloven blir utsatt for uønsket kriminell aktivitet via Internett eller mot graderte systemer vurderes å være økende.

Finanskriminalitet fra ikke-statlige aktører er vedvarende høy og økende. Kriminell aktivitet på Internett er betydelig høyere enn det antall saker som rapporteres eller anmeldes. Dette inkluderer blant annet kortsvindel, nettbankbedrageri, datainnbrudd og nettaktivisme. I 2011 etterforsket Kripos en bølge av anmeldelser for nettbankbedrageri der en utnytter innplassering av ondsinnet kode hos bankkundene.

Det er økende hyppighet og utbredelse av industrispionasje. Denne aktiviteten antas å være mer utbredt enn det som oppdages, da mange bedrifter mangler kapasitet og evne til å detektere og håndtere slike angrep. I Storbritannia ga Cabinet Office i februar 2011 ut en rapport som forsøker å kalkulere kostnadene relatert til internettkriminalitet. Omgjort til norske forhold tilsier rapporten at kostnaden for Norge beløper seg årlig til over 20 milliarder kroner.

Betegnelsen ”hacktivister” brukes om personer og grupperinger som fremmer et politisk, religiøst eller nasjonalistisk budskap gjennom forskjellig type aktivitet på Internett. De mest kjente gruppene er Anonymous og LulzSec. NSM har sett flere tilfeller av nettaktivisme i Norge gjennom 2011, for

eksempel tyveri og offentliggjøring av norske stortingspolitikeres personnummer og tjenestenektangrep mot politiske partier som støtter datalagringsdirektivet.

Terrorister har hittil vist liten interesse for å bruke IKT og Internett som en arena for terror. IKT og Internett brukes imidlerit i stort omfang som kanal for spredning og innhenting av informasjon.

4 Metoder og virkemidler

Det er grunn til å tro at fremmede stater står bak de mest kostbare og ressurskrevende metodene og virkemidlene.

Omfang og kompleksitet på spionasje ved hjelp av IKT øker stadig. Observante brukere har varslet NSM etter å ha mottatt og reagert på suspekte e-poster. Utnyttelse av sårbarheter på web- og e-postservere er vanlig. Angripere har store kapasiteter til å utvikle skreddersydd skadevare. Lavt sikkerhetsnivået i mange virksomheter muliggjør de enkleste metodene. Flere angrep har store likheter i metode og teknologi. Det er sannsynlig at samme aktør står bak flere forskjellige angrep.

Det er en endring fra tilfeldige og opportunistiske angrep til mer avanserte og fokuserte operasjoner mot spesifikke mål av høy økonomisk eller samfunnsmessig verdi. Om et angrep blir avslørt og fjernet, har angriper gjerne andre tilganger og skadevare på datasystemene som gjør at han enkelt kommer inn igjen. Kompromitteringen er dermed vedvarende. Denne adferden har blitt kalt Advanced Persistant Threat (APT) og sammenfaller med spredningen og alminneliggjøringen av avanserte verktøy.

Mulighetene for å utrette skade gjennom angrep gjennom cyberspace er potensielt store. Etter at Stuxnet ble oppdaget i 2010, spekulerte mange i om koden kunne brukes til å angripe annen infrastruktur. I november 2011 dukket Duqu opp. Duqu har fellestrekk med Stuxnet, men NSM antar at Stuxnet primært brukes til å skade infrastruktur, mens Duqu nyttes som et avansert informasjonsinnhentingsverktøy.

Spredning av avanserte verktøy er en bekymringsfull trend. Rootkits er programmer som brukes for å oppnå tilgang til et system uten av eieren er klar over det. Angriper kan på denne måten skjule sin og annen skadevares tilstedeværelse på systemet. Rootkits er blitt lettere tilgjengelig for et bredt publikum.

Antall sårbarheter oppdaget på smarttelefoner, nettbrett og lignende har vokst betydelig det siste året. Angrepsmetodene mot mobile enheter er i stor grad de samme som mot datamaskiner. Smarttelefoner er i praksis små datamaskiner, og har de samme sårbarhetene. Android-operativsystemet har blitt det mest populære målet for skadevareutviklere for mobile plattformer. Adobe-produkter har ellers blitt det mest attraktive målet for utviklere av skadevare.

Det siste året har det vært en betydelig nedgang i aktivitet fra botnets. Nedgangen knyttes særlig til en koordinert aksjon i mars for å stenge det såkalte Rustock-nettverket. I tillegg har det blant annet vært koordinerte tiltak fra nasjonale CERTer og det internasjonale sikkerhetsmiljøet.

De teknologiske mulighetene for å avlytte andre er store, og avansert avlytningsutstyr er kommersielt tilgjengelige. Smarttelefoner, lesebrett og andre mobile plattformer og lagringsmedier medfører nye sårbarheter. Alt elektronisk utstyr avgir stråling, og er dermed utsatt for informasjonsinnhenting. Metoder og utstyr er under stadig utvikling. Denne type avlytting er svært vanskelig å detektere, og legger ikke igjen spor ved tapping av et system. Mobiltelefoner kan spores, avleses eller avlyttes. Spionprogramvare og virus kan lett installeres på mobiltelefoner. I tillegg krever myndighetene i flere

land av mobiloperatørene at det er mulig å avlytte mobil- og telenettet. PST har blant annet advart mot etterretningstrusselen mot offisielle norske delegasjonsreiser.

Sosial manipulering benyttes for å påvirke mennesker til å gi fra seg sensitiv informasjon eller utføre handlinger som de normalt ikke ville ha gjort. Sosial manipulering er for eksempel svært vanlig i kombinasjon med inntrenging i informasjonssystemer. Sosial manipuleringen kan skje under direkte menneskelig kontakt eller ved elektronisk kommunikasjon, som via e-post, chat eller ved bruk av sosiale medier.

Innsider-begrepet brukes om personer som har eller har hatt autorisert tilgang til en virksomhet, og som legger til rette for at uvedkommende får uautorisert tilgang til informasjon virksomheten ønsker å beskytte. Innsidere kan være nåværende eller tidligere ansatte, eksterne konsulenter, vedlikeholdspersonell eller andre. En innsider behøver ikke selv å ha onde hensikter, men kan være sårbar overfor forledelse, overtalelse eller press.

5 Sårbarheter og sikkerhetstruende forhold

Sårbarhet betyr manglende evne til å motstå en uønsket hendelse, eller å opprette en ny stabil tilstand dersom en verdi er utsatt for en uønsket påvirkning. Sårbarheter i forhold til behandling og kommunikasjon av sensitiv informasjon forsterkes av at mange virksomheter viser utilstrekkelig risikoforståelse og har manglende kompetanse, holdninger, vilje og evne til å prioritere og å utøve forebyggende sikkerhetsarbeid.

Verdier må sikres gjennom en helhetlig tilnærming og dermed ofte med en kombinasjon av teknologiske, organisatoriske og menneskelige barrierer eller sikkerhetstiltak. Menneskelige faktorer som kunnskap, kompetanse, vilje, forståelse og holdninger må være på plass som et premiss for at organisatoriske og tekniske aspekter ved sikkerhetsarbeid skal fungere. I fravær av menneskelige sikkerhetsrelaterte egenskaper, vil menneskelig sårbarheter kunne påvirkes og manipuleres av trusselaktører.

Disse forholdene representerer en sårbarhetsutfordring som kan utnyttes av en trusselaktør. Sikkerhetstruende forhold er vurdert opp mot at fremmede staters etterretningstjenester eller spesialavdelinger er den dimensjonerende trusselaktør.

Tekniske sårbarheter finnes i alle typer IKT-programvare og operativsystemer. Sikkerhetshull kan utnyttes gjennom ondsinnet aktivitet. De mest verdifulle sikkerhetshullene for en trusselaktør vil være de som produsentene av systemene enda ikke har kjennskap til eller har utviklet koder for å tette svakhetene til.

Teknikkene for å angripe IT-systemer blir stadig mer avanserte og til en viss grad mer målrettede. Begrepet ”malware”, er en sammenslåing av ordene ”malicious” og ”software”. På norsk brukes også begrepet skadevare. Dette er kjørbar programkode som er utviklet for å utføre skjulte eller skadelige handlinger på infiserbare systemer. Skadevare kan true tilgjengelighet, integritet og konfidensialitet[1] i et informasjonssystem.

[1] Tilgjengelighet: det at du får tak i den informasjon du søker. Integritet: det at informasjonen ikke er manipulert. Konfidensialitet: det at uvedkommende ikke får tilgang til informasjonen.

Angrep via Internett kan deles i to kategorier. Den første kategorien er nettverksbaserte angrep, det vil si angrep mot tjenester på klienter og servere som normalt ikke krever interaksjon fra en bruker. Den andre kategorien er såkalte ”client-side” angrep som retter seg mot programvare som er installert på brukerens datamaskin. Denne typen angrep krever normalt at brukeren utfører en handling – for eksempel klikker på en link i en e-post, eller åpner et vedlegg – før angrepet kan lykkes. I slike tilfeller vil kartlegging av målet være en viktig del av forberedelsene til angrepet. I de tilfeller sistnevnte angrep utføres målrettet vil standard sikkerhetsprogramvare ha vanskelig for å oppdage og avverge angrepet.

Skadevare som oppdages på Internett kan også bli brukt mot graderte eller lukkede systemer. Dette kan for eksempel skje ved hjelp av innsidere som får tilgang til og manipulerer eller infiserer slike systemer, eller ved at skadevaren infiserer lukkede systemer ved bruk av USB minnepinner.

Det er kjent at en mengde gradert informasjon er tilgjengelig på Internett, enten lagt ut bevisst eller på grunn av ubevisste handlinger. Slik informasjon kan identifiseres og utnyttes med negativ intensjon av trusselaktører.

Det er en stor fare for at trusler mot ugraderte systemer også kan kompromittere skjermingsverdig informasjon.

5.1 Risikoforståelse

Mange virksomheter har mangelfull sikkerhetsmessig risikoforståelse

NSM registrerer ofte mangler i forhold til ledelsens plikt til å ha oversikt over egen sikkerhetstilstand basert på risikovurderinger.

Dette får sitt uttrykk gjennom manglende kartlegging av, liten forståelse for, og lav bevissthet om, hvilke verdier virksomhetene har behov for å skjerme, hvilke trusler verdiene står overfor, og hvilke sårbarheter som kan utnyttes og derfor må forebygges mot. Basert på tilsyn og annen empiri er det NSMs vurdering at virksomhetenes ledelse gjennomgående feilvurderer sikkerhetstilstanden i egen virksomhet.

Manglende bevissthet om at mennesker, informasjon, utstyr og funksjoner har en verdi for virksomheten eller for samfunnet, fører ofte til ukontrollert spredning av informasjonen og tap av verdier. Informasjon om spesifikke og alvorlige sårbarheter av samfunnsmessig betydning kan bli tilgjengeliggjort og utnyttet av trusselaktører gjennom sabotasje- eller terrorhandlinger. Dette kan føre til reduksjon i, eller ødeleggelse av, kritiske samfunnsfunksjoner og infrastrukturer, og dermed undergrave samfunnets fundamentale verdier. Samfunnets samhandlingsevne og tjenester som styres av IKT kan svekkes.

Manglende risikovurdering vil i tillegg kunne medføre feil prioritering av hva som må beskyttes og feil nivå på sikkerhetstiltakene. Når sikkerhetstruende forhold ikke umiddelbart utbedres, medfører dette en utvidet sårbarhet som i enda høyere grad kan utnyttes av trusselaktører.

5.2 Ledelsesoppfølging

Virksomhetsledere følger ikke opp sikkerhetsarbeidet

Virksomhetsledere[2] er pålagt å evaluere eget sikkerhetsarbeid årlig. Normalt etterspør de imidlertid ikke informasjon om forebyggende sikkerhet, og de er sjelden involvert i evaluering av sikkerhetsarbeid eller resultatrapportering. Dette er aktiviteter som ofte ikke blir gjennomført.

Det eksisterer sjelden etablerte systemer for at virksomhetsleder skal bli informert eller varslet om sikkerhetsbrudd og sikkerhetstruende hendelser.[3] Ved tilsyn konstaterer NSM i praksis alltid at det har foregått eller foregår sikkerhetstruende hendelser, som virksomhetene ikke har oppfattet eller registrert. Dermed er muligheten til å korrigere og forbedre eget sikkerhetsarbeid fraværende. Egen og andres virksomhet utsettes for unødig risiko ved at det unnlates å rapportere sikkerhetstruende hendelser og sikkerhetsbrudd. Omfanget av sikkerhetstruende virksomhet blir vanskelig å beregne, det blir vanskelig å utvikle relevante sikkerhetstiltak og det blir enklere for trusselaktører å lykkes med sine aktiviteter.

Dersom sikkerhetsorganisasjonen mangler tilgang til og/eller har stor avstand til virksomhetsledelsen kan dette føre til at sikkerhetsmessige utfordringer ikke blir håndtert og at sikkerhetsmessige akuttsituasjoner får unødvendig store negative konsekvenser. Når ressurser dedikert til sikkerhet mangler, blir det begått bevisste og ubevisste sikkerhetsbrudd som øker sikkerhetsrisiko og sårbarhet.

Det fins flere tilfeller der virksomhetsledelsen av forskjellige grunner har nedprioritert nødvendige sikkerhetsmessige oppdateringer eller godkjenninger av IKT-systemer. Dette vanskeliggjør sikkerhetsleders eller datasikkerhetsleders oppgaveutførelse. Manglende sikkerhetsgodkjenning av systemer og sammenkoblinger medfører ofte at beskyttelsestiltak ikke er tilstrekkelige.

Overordnet virksomhet etterspør ikke rapportering om sikkerhetsarbeidet fra underordnet virksomhet. Da får de det ikke. Manglende oversikt over sikkerhetstilstanden i underlagte ledd kan føre til at sårbarheter lettere kan utnyttes av trusselaktører.

I flere tilfeller har NSM gjort observasjoner som tyder på at virksomhetene bevisst ikke etterlever sikkerhetsloven med forskrifter fullt ut. Dette gjelder blant annet reglene knyttet til sikkerhetsgradering av informasjon og gjennomføring av øvelser innen forebyggende sikkerhet.

5.3 Sikkerhetskultur, -kunnskap og –holdninger

Slapp sikkerhetskultur og dårlige kunnskaper

Det er NSMs vurdering at kompetansen hos sikkerhetspersonell har vært nedadgående de senere årene. Mange ledere, og ofte personell tillagt konkrete sikkerhetsoppgaver, mangler kompetanse om hvordan oppgaver tilknyttet forebyggende sikkerhet skal eller kan løses. Dette fører ofte til sikkerhetsbrudd som begås i god tro.

Dette har som regel sammenheng med mangel på planmessig opplæring i virksomheten. I tillegg kan det ofte ha sammenheng med høy utskiftingsgrad av personell, samtidig som intern erfaringsoverføring synes å være utilstrekkelig. Høy utskiftningsgrad brukes gjerne som forklaring når det avdekkes at personell ikke er gitt anledning til å skaffe seg nødvendig kompetanse.

[2] I virksomheter underlagt sikkerhetsloven.

[3] NSM har i 2011 etablert en link på sin hjemmeside, hvor det informeres om hva som skal rapporteres, og til hvem og hvordan.

Det ble eksempelvis i ett tilfelle hvor en intern instruks om sikkerhetstjeneste var trådt i kraft, konstatert at instruksen ikke var tatt i bruk i virksomheten. Dette førte blant annet til at sikkerhetstruende hendelser ikke ble rapportert som forutsatt. I virksomheter der sikkerhetsbrudd begås uten at dette rapporteres og følges opp, vil sikkerhetskulturen kunne bli svekket. Manglende sikkerhetskultur kan føre til at risikoatferd opprettholdes, at ledelsen ikke har oversikt over sikkerhetstilstanden og at sannsynligheten for kompromitteringer og alvorlige hendelser øker.

Når sikkerhetskultur, kunnskap og kompetansen mangler, er sannsynligheten større for at det blir begått sikkerhetsbrudd, noe som i seg selv skaper sikkerhetsrisiko og sårbarhet. Dette vil igjen legge til rette for at trusselaktører kan realisere sine mål ved bruk av enklere og mindre kapasitetskrevende metoder og virkemidler enn de ellers ville ha måttet benytte.

5.4 Styringssystem for sikkerhet

Manglende styring av sikkerhetsarbeidet

Virksomhetenes styringssystemer inkluderer ofte ikke forebyggende sikkerhet, og systemer for kvalitets- og risikostyring på dette området er til dels fraværende. Det er mangelfull dokumentasjon av eget sikkerhetsarbeid. Dokumentasjon bærer gjerne preg av å ha blitt opprettet rett før et tilsyn og ofte gjentas kun krav i lov og forskrift. Kravene er gjerne ikke operasjonalisert og heller ikke gitt en løsning forankret i lokale forhold. Dette tyder på at dokumentasjonen ikke er knyttet til det daglige virket.

Både sikkerhetsloven og andre regelverk forutsetter internkontroll eller andre typer kvalitetssystemer, hvor det er et prinsipp at utøvende og kontrollerende roller skal skilles i virksomheten. For forebyggende sikkerhet blandes ofte disse rollene.

Manglende styringssystem og dokumentasjon for sikkerhet fører til at

- virksomhetens oppfølging av det forebyggende sikkerhetsarbeidet ikke ivaretas på en systematisk og god måte
- virksomheters mulighet for forbedring og læring svekkes
- sikkerhetsarbeidet blir preget av tilfeldigheter og oppdukkende behov
- det blir vanskeligere å kontrollere sikkerhetsarbeidet opp mot regelverket
- kvaliteten på sikkerhetsarbeidet, herunder grad av kravs- og måloppnåelse, blir utilstrekkelig belyst
- det ikke blir mulig å måle årlig utvikling
- sikkerhetsarbeid ikke tas hensyn til for gjennomføring og etterlevelse
- det blir vanskelig å gi pålegg om utbedring, og å vite om tiltak er formålstjenlig innrettet i forhold til det faktiske risikobildet.

Dersom alle virksomheter, sektoretater og departementer hadde klarere pålegg om å rapportere målbare fakta og trender hva angår intern og sektoriell sikkerhetstilstand, ville både NSM og de konstitusjonelt ansvarlige ha et bedre grunnlag for utarbeidelse av formålstjenlig politikk og beslutningsgrunnlag innen forebyggende sikkerhet og tiltak.

5.5 Personellsikkerhet og autorisasjon av virksomheter

Sikkerhetsutfordringer rundt personellsikkerhet og autorisasjon av personer og virksomheter

Personell må sikkerhetsklareres før de autoriseres og gis tilgang til informasjon sikkerhetsgradert KONFIDENSIELT eller høyere. Virksomhetens ledelse forstår ofte ikke forskjellen på klarering og autorisering og tror derfor at klarering er tilstrekkelig. Virksomhetene unnlater derfor ofte å autorisere

personell for tilgang til sikkerhetsgradert informasjon. Særlig private virksomheter har problemer med å sikre at daglig leder er autorisert.

Dersom personellsikkerhetsprosessene ikke følges, innebærer det eksponering av store sårbarheter, hvor konsekvensen kan bli at personer som utgjør eller vil kunne utgjøre en risiko vil kunne få tilgang til sensitiv og skjermingsverdig informasjon, som igjen kan lede til alvorlig ondsinnet virksomhet mot norske interesser.

Virksomhetsautorisasjon er et viktig tiltak i forhold til organisering, evne til å holde oversikt over og kontroll med underlagte virksomheter. I tillegg er det et virkemiddel for å sette disse i stand til og forstå hvordan gradert informasjon skal behandles.

Offentlige virksomheter unnlater ofte å autorisere underlagt virksomhet, og mangler oversikt over autorisasjoner. Virksomhetens autorisasjon vil normalt være styrende for hvorvidt det kan fremmes anmodning om personkontroll og på hvilket nivå en kan få en person sikkerhetsklarert.

NSM har registrert flere tilfeller hvor personell som ikke er autorisert likevel har tilgang til sikkerhetsgradert informasjon. Dette kan være på systematisk basis via arbeidsoppgaver, eller mer tilfeldig, ved at fysisk tilstedeværelse på arbeidsplassen gir mulighet for tilgang. Når personer som ikke er autorisert har fått tilgang til sikkerhetsgradert informasjon, uten at det finnes noen dokumentert oversikt over spesifikke tilgangsgrupper, anses denne informasjonen som kompromittert.

5.6 Dokumentsikkerhet og beredskap mot sikkerhetstruende hendelser

Problematisk å holde oversikt over graderte dokumenter, særlig i kritiske situasjoner

Virksomhetene har ofte mangelfull oversikt over og kontroll over graderte dokumenter, slik at man risikerer at disse kompromitteres uten at det oppdages, uten at det lar seg gjøre å finne ut av årsaken eller uten å kunne vurdere eventuelle skadevirkninger.

Virksomhetene har ofte heller ikke dokumentert evne til å håndtere graderte dokumenter og annet gradert materialeunder sikkerhetstruende hendelser. Når ukjente mengder graderte dokumenter er spredt på saksbehandlere utenom arkivets kontroll, blir arkivsanering og eventuell evakuering eller nødmakulering vanskelig- eller umuliggjort i en krisesituasjon.

Risiko- og sårbarhetsanalyser (ROS) i forhold til kontinuitetsplanlegging er ofte for enkle, da de ikke omfatter kontinuitet av et sikkerhetsregime.

Mange steder er sikkerhetsrelaterte beredskapsplaner mangelfulle. Det finnes vanligvis bare beredskapsplaner på krypto-området, men disse er ofte ikke tilstrekkelige. Det avdekkes ofte at beredskapstiltak tilknyttet ivaretagelse av sikkerhet i situasjoner med forhøyet risiko ikke er øvd årlig slik regelverket krever. Sikkerhetsmessige tiltak som skal iverksettes ved beredskap, krise eller krig blir ikke planlagt, utarbeidet og testet.

I politi- og militæroperasjoner kan manglende dokumentsikkerhet og sikkerhetsmessig beredskap gjøre at taktiske og operasjonelle forhold blir gjort kjent for uvedkommende, noe som kan lette ondsinnede aktørers evne til å påføre skade på mennesker og utstyr.

5.7 Fysisk sikring

Lås døren og slå på alarmen!

NSM finner at flere virksomheter mangler klart definerte og avgrensede områder for behandling av gradert informasjon og har mangler i forhold til låsing og alarmering. I mange tilfeller der det er installert innbruddsalarmanlegg er disse ikke underlagt jevnlig funksjonskontroll og ettersyn. Ved mange virksomheter er det ikke vakthold utenom normal arbeidstid.

5.8 Lokaler for sikkerhetsgraderte samtaler

Det er for mye gradert tale på uegnede steder

Sikkerhetsgraderte samtaler på høyere graderingsnivå skal kun finne sted i rom som er tilstrekkelig sikret og godkjent for dette formålet. Slike rom er det for få av. Dette fører til mulige sikkerhetsbrudd når graderte samtaler likevel finner sted utenfor slike rom og i områder som man har dårlig kontroll over. Dette gjør det relativt enkelt for mulige trusselaktører å avlytte samtaler eller for eksempel å avlese presentasjoner.

5.9 Leverandører av sikkerhetsgraderte anskaffelser

Økende sårbarhet innen leverandørkjeden og industrisikkerhet

En anskaffelse er sikkerhetsgradert dersom den medfører at leverandøren får utlevert eller vil tilvirke gradert informasjon. Det er den enkelte anskaffelsesmyndigheter som er ansvarlig for regelmessig å kontrollere sikkerhetstilstanden hos leverandører av sikkerhetsgraderte anskaffelser. Det er registrert alvorlige sårbarheter hos virksomheter som leverer samfunnskritiske tjenester. Disse sårbarhetene kan bli, og har blitt, avdekket og utnyttet på en måte som kan få store sikkerhetspolitiske og/eller økonomiske konsekvenser.

5.10 IKT-sikkerhet

IKT-systemer har ofte store sikkerhetsmessige svakheter

Samfunnet baserer seg i økende grad på digitale løsninger for kommunikasjon, oppbevaring av informasjon og styring av viktige prosesser. Uønsket aktivitet over Internett utgjør risiko for stor skade mot Norge og norske interesser.

NSM er bekymret for sikkerheten i samfunnskritiske informasjonssystemer. Både i sivile sektorer og militær sektor har inntrengingstesting påvist svært alvorlige svakheter. Dette er svakheter som har kunnet gi en trusselaktør tilgang til, og mulighet til å manipulere, endre og slette, både svært sensitiv informasjon og høyt gradert informasjon.

Virksomhetene klarer ofte ikke å vedlikeholde sikkerheten i forhold til IKT-systemer på en tilfredsstillende måte. De implementerer gjerne ikke krav til sikkerhet slik det fremgår av virksomhetens egne styrende dokumenter. På en rekke områder er det store avvik mellom vedtatte krav og faktisk sikkerhetstilstand i systemene.

Det er ofte store uoverensstemmelser mellom informasjonssystemets dokumentasjon og den reelle implementerte tilstanden. Dette gjør seg spesielt gjeldende i form av enheter i nettverket som det ikke er redegjort for, og derfor heller ikke er kjente for personellet som vedlikeholder systemet. Dette

omfatter både enheter som skal være der, som printere og telefoner, og enheter som ikke hører hjemme der, for eksempel privat utstyr. Når brukere tillates nedlastingsmuligheter for programvare, kan det finnes programvare på virksomhetens IKT-systemer som administrator ikke vet om. Dette er i verste fall skadevare. I beste fall har ikke administrator mulighet til å holde dette sikkerhetsmessig oppdatert.

Mange virksomheter mangler grunnleggende kontroll over dataflyten i egne nettverk. I mange virksomheter er kunnskapen om hvorfor en kontrollert dataflyt er nødvendig fraværende. Manglende sikkerhetsmekanismer fører ofte til at servere er unødvendig eksponert og potensielt åpne for angrep. I enkelte tilfeller har NSM også observert manglende segregering mellom virksomhetens interne nettverk og for eksempel gjestenettverk. Det har blitt observert systemer hvor kritisk intern infrastruktur har vært sårbar for angrep fra en trusselaktør tilknyttet åpne gjestenett, også trådløse.

Det fins ofte store svakheter når det gjelder sikkerhetsmessig oppdatering av kritiske og sikkerhetsgraderte informasjonssystemer. Dette gjelder både for operativsystemer og programvare på klientmaskiner, kritiske servere og annen teknisk infrastruktur. Disse manglene medfører ofte svært stor risiko for kompromittering. NSM har observert kritiske servere i samfunnskritiske informasjonssystemer som ikke har vært oppdaterte på flere år. I tillegg har man i flere tilfeller observert servere som benytter seg av programvare og operativsystemer som ikke lenger støttes av leverandør og hvor det ikke finnes oppdateringer.

Typiske avvik i administrasjonen av alle typer IKT-systemer er: 1) manglende sikkerhetsoppgradering (patching), 2) mangelfull passordadministrasjon, testing av ny programvare eller applikasjon uten å fjerne testapplikasjonen og logg-on til den etterpå, 3) mangelfull fjerning av gamle versjoner ved oppdateringer, 4) manglende oppmerksomhet på tidsbegrensinger i antivirus-programvare[4] og 5) manglende begrensninger i brukernes muligheter til å laste ned tredjeparts programvare.

Passordsikkerheten i enkelte testede systemer har vist seg å være svært svak. NSM har i flere testede systemer funnet et større antall brukere med svake passord. I tillegg har det blitt observert domeneadministratorbrukere i flere større og samfunnskritiske systemer med svake passord.

Grunnet mangelfull logging er det ikke mulig å si noe om hva slags og hvor mye data som har gått tapt.

All informasjon i IKT-systemer uten tilstrekkelige og oppdaterte sikkerhetstiltak kan potensielt avleses, fjernes eller endres uten at det oppdages. Uobservert fysisk tilgang til datamaskiner gir oftest mulighet for uautorisert inntrengning i maskinene, med tap av konfidensialitet og integritet på informasjonen som følge.

NSM har observert at det i svært liten grad benyttes diskkryptering på klientmaskiner. I tillegg benyttes det ofte svake krypteringsmekanismer for lokalt lagrede passord på slike maskiner. Hvis slike enheter mistes, glemmes eller stjeles, kan dette gi uvedkommende tilgang til informasjon som er lagret på maskinen, og potensielt også til virksomhetens nettverk.

5.11 Tempestsårbarheter

Vær oppmerksom på elektronisk avlyttingsrisiko

Tempest er en betegnelse på stråling i form av radiosignaler fra et IKT-system. Det er ingen krav til Tempest-beskyttelse av systemer som behandler ugradert informasjon. Mesteparten av det IKT-

[4] Nyere versjoner av programvaren stopper ofte ikke gammel og antatt ukurant skadevare

utstyret som selges i dag avgir avlyttbar stråling og må kontrolleres for dette før det tas i bruk for gradert informasjon.

Krav om å Tempestsikre gjelder for objekter som har installert informasjonssystemer for sikkerhetsgradert informasjon. Det stilles krav til gjennomføring av Tempest-risikovurdering for systemer som skal behandle sikkerhetsgradert informasjon i Norge og i utlandet. For installasjoner i Norge er det ikke krav til å Tempest-beskytte informasjonssystemer som behandler BEGRENSET informasjon.

Ved å etablere fysisk avstand til en mulig avlytter, vil Tempestrisikoen, og krav til tiltak som må iverksettes, reduseres.

5.12 Kryptosikkerhet

Uheldig tendens i utviklingen av kryptoteknologi

Kontinuerlig innovasjon og modernisering er nødvendig for å ivareta kryptosikkerhet over tid. Det vil også være avgjørende at man utvikler og videreutvikler produkter og kapasiteter etter hvert som man ser at trusselbildet endres grunnet endrede bruksmønstre og bruksområder. Kryptosystemer har spesielt strenge sikkerhetskrav og skal ha særlig godkjenning.

Mangel på kryptoutviklingsprosjekter fører til færre ansatte med kryptokompetanse hos norsk kryptoindustri. NSM er bekymret for utviklingen når det gjelder grunnleggende kryptoinfrastruktur.

Fortsetter utviklingen, er det risiko for at høygradert skjermingsverdig informasjon blir kompromittert og dermed utsatt for utnyttelse av ondsinnede trusselaktører.

Nasjonal sikkerhetsmyndighet