Nasjonal sikkerhetsmyndighet

Veiledning
Sist oppdatert: 2016-03-09

Veiledning i planlegging av graderte informasjonssystemer

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er tverrsektoriell fag- og tilsynsmyndighet innenfor forebyggende sikkerhetstjeneste i Norge og forvalter lov om forebyggende sikkerhet av 20. mars 1998. Hensikten med forebyggende sikkerhet er å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, primært spionasje, sabotasje og terrorhandlinger. Forebyggende sikkerhetstiltak skal ikke være mer inngripende enn strengt nødvendig, og skal bidra til et robust og sikkert samfunn.

Hensikt med veiledning

NSM sin veiledningsvirksomhet skal bygge kompetanse og øke sikkerhetsnivået i virksomhetene, gjennom økt motivasjon, evne og vilje til å gjennomføre sikkerhetstiltak. NSM gir jevnlig ut veiledninger til hjelp for implementering av de krav sikkerhetsloven stiller. NSM publiserer også veiledninger innen andre fagområder relatert til forebyggende sikkerhetsarbeid.

Postadresse
Postboks 814
1306 SANDVIKA

Sivil telefon/telefax
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09

Internettadresse
www.nsm.stat.no

Innhold

1 Beskrivelse

Når en virksomhet skal ta frem et informasjonssystem som skal behandle, lagre og transportere gradert informasjon er det mange vurderinger som må gjøres på forhånd. Å ta frem en slik løsning skal følge en planlagt, strukturert og dokumentert prosess, slik at nødvendig og tilstrekkelig sikkerhet blir ivaretatt i hele informasjonssystemets levetid. Formålet med denne veiledningen er å veilede virksomhetene gjennom forholdene som er særskilte for graderte informasjonssystemer og de avklaringene som må gjøres for å planlegge denne prosessen, slik at de har et best mulig utgangspunkt for det videre arbeidet med sikkerhet. Disse avklaringene skal dokumenteres og det er naturlig at dette gjøres gjennom å utarbeide et sikkerhetskonsept[1]. Veiledningen berører kun den innledende planleggingsfasen, for man setter i gang med anskaffelse eller utvikling av informasjonssystemet.

Et sikkerhetskonsept er en overordnet beskrivelse av informasjonssystemets funksjon og miljø, brukere, verdien av informasjonen som skal behandles, systemets omfang og kompleksitet og eventuelle eksterne tilkoblinger. Denne veiledningen beskriver en del forhold virksomheten må ta stilling til for å danne grunnlaget for utarbeidelsen av et sikkerhetskonsept.

NSM har veiledere på flere av områdene som omtales i dette dokumentet.

2 Målgruppe

Veilederen er beregnet for alle virksomheter underlagt sikkerhetsloven som planlegger å anskaffe, utvikle eller oppgradere et gradert informasjonssystem.

[1] Forskrift om informasjonssikkerhet § 5-33 stiller krav om at det skal utarbeides et sikkehetskonsept for alle graderte informasjonssystemer.

3 Definisjoner

Begrep	Forklaring
Brukersted	Virksomhet eller avdeling av virksomhet som til daglig benytter informasjonssystemet
Brukerstedsgodkjenning	Godkjenning av et informasjonssystem brukt i en virksomhet på en gitt lokasjon
Driftsansvarlig	Ansvarlig for den daglige driften av informasjonssystemet, tjenesteleverandør
Driftsgodkjenning	Godkjenning av driftsløsningen for et informasjonssystem
Driftsløsning	Informasjonssystem hos driftsansvarlig, i tillegg til prosedyrer og rutiner som skal ivareta sikker drift og vedlikehold av informasjonssystemet.
Evaluering	Teknisk vurdering som har til hensikt å påvise om systemtekniske sikkerhetstiltak har den nødvendige tilliten.
Evalueringsrapport	Rapport fra tredjepart etter gjennomført sikkerhetsevaluering av produkt eller informasjonssystem
Referansegodkjenning	Godkjenning av referanseløsning for et informasjonssystem
Referanseløsning	Systemteknisk konfigurasjon, arkitektur og prosesser for et informasjonssystem
Samsvarserklæring	Erklæring på at man oppfyller krav i henhold til sikkerhetsloven med forskrifter, samt andre nærmere angitte krav i NSMs veiledere
Sertifisering	Typegodkjenning av produkt eller løsning basert på en evaluering.
Sikkerhetsgodkjenning	Avgjørelse om at et informasjonssystem i en virksomhet tillates brukt til behandling, lagring eller transport av sikkerhetsgradert informasjon. Kan deles opp i referansegodkjenning, driftsgodkjenning og brukerstedsgodkjenning.
Systemteknisk sikkerhet	Sikkerhet som ivaretas i og av informasjonssystemets program- og maskinvare
Tjenestenivåavtale	Avtale mellom leverandør og kunde som sier noe om forventet nivå på tjenestene som leveres (SLA – eng. Service Level Agreement)

4 Sikkerhetskonsept

Sikkerhetskonseptet skal beskrive det planlagte informasjonssystemet på et overordnet nivå. Kapitlene videre i denne veilederen beskriver hvordan krav til sikkerhetskonsept kan oppfylles. Sikkerhetskonseptet skal tilpasses hvert enkelt systems størrelse og kompleksitet. Hvem som er godkjenningsmyndighet avgjøres på bakgrunn av sikkerhetskonseptet. Konseptet danner også grunnlaget for godkjenningsstrategien. Det er vesentlig at man så tidlig som mulig i prosessen med å ta frem et informasjonssystem som skal sikkerhetsgodkjennes utarbeider et utkast til sikkerhetskonsept som grunnlag for dialog med godkjenningsmyndighet og øvrige interessenter. Det er mulig å revidere sikkerhetskonseptet helt frem til sikkerhetsgodkjenning gis. Sikkerhetskonseptet er et sentralt grunnlag for sikkerhetsgodkjenning av informasjonssystemet og endringer i sikkerhetskonseptet vil kreve ny sikkerhetsgodkjenning.

NSM anbefaler at sikkerhetskonseptet holdes konsist og ikke overstiger 5-10 sider, avhengig av informasjonssystemets kompleksitet og størrelse.

Sikkerhetskonseptet kan med fordel tas frem som en del av, eller vedlegg til, den øvrige konsept-dokumentasjonen i forbindelse med planleggingen av informasjonssystemet.

De neste kapitlene beskriver en del forhold virksomheten må ta stilling til for å danne grunnlaget for utarbeidelsen av et sikkerhetskonsept.

Kapittel 15 og 16 beskriver forhold knyttet til selve sikkerhetsgodkjenningen.

5 Roller og ansvar

Ansvarsforhold må avklares så tidlig som mulig i prosessen med å ta frem et gradert informasjonssystem. Disse rollene skal dekke hele livsløpet til informasjonssystemet. Rollene NSM finner naturlig å bruke er utviklingsansvarlig, driftsansvarlig og brukerstedsansvarlig for det aktuelle informasjonssystemet. Rollene kan fordeles på flere virksomheter, eller legges til samme virksomhet, men for eksempel til forskjellige avdelinger eller enheter. Dette vil avhenge av organisatoriske forhold og størrelsen og kompleksiteten på arbeidet med å anskaffe eller drifte systemet. Rollene kan også deles opp på en annen måte enn det som er beskrevet i denne veilederen, om det er mer hensiktsmessig.

Med disse rollene menes ikke enkeltpersoner, men organisatoriske enheter som innehar definert ansvar. Dette kan være separate virksomheter eller fordelt internt i en virksomhet, for eksempel ved at en IKT-avdeling er delt i en enhet for drift og en enhet for utvikling og forvaltning.

5.1 Systemeier

Begrepet «systemeier» benyttes i forskrift om informasjonssikkerhet, men er ikke definert i forskriften. NSM erfarer at ulike virksomheter legger forskjellig innhold i begrepet. NSM ønsker derfor å gå bort fra bruken av dette. Ansvaret en systemeier skal ha i henhold til sikkerhetsloven er dekket gjennom rollene beskrevet ovenfor. Det må være tydelig avklart mellom virksomhetene hvem som har hvilket ansvar. Disse rollene erstatter således systemeier i denne veilederen.

5.2 Utviklingsansvarlig

Utviklingsansvarlig er den som har ansvar for å utvikle informasjonssystemet. Det vil være utviklingsansvarlig som skal utlede systemtekniske sikkerhetskrav fra NSMs teknologiveiledere på bakgrunn av sikkehetskonseptet, definere sikkerhetstiltak som møter kravene og utvikle nødvendige

test- og verifikasjonsplaner for å sikre at sikkerhetstiltak er implementert. Videre skal utviklingsansvarlig holde dokumentasjonen oppdatert når endringer gjøres i referanseløsningen

Ved større informasjonssystemer som skal benyttes på mange ulike brukersteder er det vanlig at utviklingsansvarlig først søker om en såkalt referansegodkjenning for informasjonssystemet. Utviklingsansvarlig er ansvarlig for sikkerhetsdokumentasjonen som skal produseres i forbindelse med referansegodkjenning av informasjonssystemet og skal stille krav til informasjonssystemets bruks- og driftsansvarlig.

Det er utviklingsansvarlig som normalt skal avtale en godkjenningsstrategi med godkjenningsmyndigheten. Dersom driftsansvarlig og brukersted er andre virksomheter bør de også involveres i dette arbeidet.

5.2.1 Forvalter

I de tilfellene hvor utviklingsansvarlig ikke er ansvarlig for den videre forvaltningen etter at informasjonssystemet er utviklet må denne rollen defineres. Forvalter er ansvarlig for feilretting og oppdatering av teknisk utstyr og programvare, endring av konfigurasjon og funksjonalitet, samt å oppdatere sikkerhetsdokumentasjonen for å reflektere disse endringene.

Den som forvalter informasjonssystemet er ansvarlig for å opprettholde informasjonssystemets referansegodkjenning.

Oppdatering av teknisk utstyr, programvare, endring av konfigurasjon og funksjonalitet kan gjøres innenfor rammene av samme referansegodkjenning dersom informasjonssystemets sikkerhetskonsept legger til rette for det. Sikkerhetskonseptet bør ta høyde for de endringer og oppdateringer som det forventes behov for å gjøre innenfor informasjonssystemets levetid, som for eksempel sikkerhetsoppdateringer og patching av informasjonssystemet.

5.3 Driftsansvarlig

Driftsansvarlig er ansvarlig for den daglige driften av informasjonssystemet, og er således den som leverer IKT-tjenester til brukerstedet. Driftsansvarlig har ansvar for å ivareta sikker drift og vedlikehold av informasjonssystemet, samt deteksjon og hendelseshåndtering. Kravene til driftsansvarlig utledes fra den overordnede sikkerhetsdokumentasjonen som tas frem av utviklingsansvarlig.

Driftsansvarlig skal så tidlig som mulig fastsette hvilke ressurser som er nødvendige for det daglige sikkerhetsarbeidet.

Driftsansvarlig skal jevnlig gjennomføre sikkerhetsrevisjon for å verifisere sikkerhetstiltak innen sitt ansvarsområde for å sikre at sikkerhetstiltak er implementert og virker i henhold til kravene. Det kan også være hensiktsmessig at driftsansvarlig avtaler med brukerstedsansvarlig rett til å gjennomføre sikkerhetsrevisjoner eller på annen verifisere at sikkerheten er tilstrekkelig ivaretatt på brukersted.

5.4 Brukerstedsansvarlig

Brukerstedet til et informasjonssystem er de virksomhetene som til daglig benytter seg av systemet. Brukerstedsansvarlig er ansvarlig for å innføre lokale sikkerhetstiltak (fysiske, administrative, personellmessige og TEMPEST) på brukerstedet og skal formelt akseptere restrisikoen i informasjonssystemet før det søkes om sikkerhetsgodkjenning. Brukerstedsansvarlig bør sørge for å inngå en avtale med driftsansvarlig om nivået på tjenestene som leveres, en såkalt tjenestenivåavtale/Service Level Agreement (SLA). Tjenestenivåavtalen må også ivareta nødvendige krav til sikkerhet i leveransene, samt brukerstedsansvarliges rett til å verifisere at tilstrekkelige sikkerhetstiltak er på plass.

Når brukerstedet skal søke om bruksgodkjenning for en lokal installasjon av et informasjonssystem må lokale forhold ved virksomheten dokumenteres, samt hvordan eventuelle avvik fra krav i den overordnede dokumentasjonen er håndtert.

Brukerstedsansvarlig skal gjennomføre sikkerhetsrevisjoner innenfor sitt ansvarsområde for å sikre at lokale sikkerhetstiltak er i henhold til kravene.

6 Verdivurdering

En verdivurdering skal hjelpe virksomheten å få oversikt over informasjon og objekter som om de kompromitteres vil få konsekvenser for virksomhetens måloppnåelse, rikets sikkerhet og selvstendighet eller andre interesser. Vurderingen bør ta utgangspunkt i hvilken skade en kompromittering vil kunne medføre i ytterste konsekvens.

Verdivurderingen bør nyanseres, slik at den tar hensyn til informasjonens autentisitet, integritet, tilgjengelighet og konfidensialitet. Konsekvensene ved sammenstilling av informasjon som er tilgjengelig i informasjonssystemet må også vurderes. Hvis det finnes store mengder sikkerhetsgradert informasjon i et informasjonssystem skal hele eller deler av informasjonssystemets infrastruktur skal sikres som om det inneholdt informasjon gradert ett nivå høyere informasjon.

Dersom informasjonssystemet lagrer eller behandler flere forskjellige organisasjonsenheters eller virksomheters graderte informasjon må de ulike informasjonseierne identifiseres og disse må involveres i verdivurderingen. Dersom informasjonssystemet lagrer eller behandler NATO-gradert informasjon må dette også tas hensyn til under verdivurderingen.

Varighet på graderingen må også tas med i betraktningen. Dersom all informasjonen i informasjonssystemet kun anses for å være gradert i kortere perioder vil dette kunne muliggjøre tilpasning av krav for ivaretakelse av konfidensialitet.

7 Sikkerhetsklarering og autorisasjon

Det er krav til autorisasjon av alle brukere som skal ha tilgang til informasjonssystemer som behandler gradert informasjon. Dersom systemet er gradert KONFIDENSIELT eller høyere, skal den enkelte bruker på forhånd være sikkerhetsklarert for minimum samme nivå.

Med mindre informasjonssystemet har dedikert operasjonsmåte skal administratorer eller brukere med utvidede rettigheter klareres for minst ett nivå høyere enn graderingen på informasjonen i systemet. Dette gjelder der brukere har mulighet til å gi seg selv ytterligere rettigheter, slå av varslingsfunksjoner, skjule spor etter aktivitet gjennom å endre logger eller å hente ut sammenstilt informasjon med høyere graderingsnivå på tvers av systemets autorisasjonsskiller.

Dersom informasjonssystemet skal behandle NATO-graderinger eller andre typer koalisjonsgraderinger, må brukerne også være sikkerhetsklarert og autorisert på tilsvarende NATO-nivå og eller koalisjonsnivå.

8 Operasjonsmåte

Operasjonsmåter benyttes for å gruppere informasjonssystemene ut i fra brukernes klarering, autorisasjon og tjenstlige behov (need to know). Det finnes fire operasjonsmåter: dedikert, fellesnivå, partisjonert og flernivå. Figuren på neste side viser hvordan man finner operasjonsmåten til et informasjonssystem.

Har alle brukere:			Operasjonsmåte
Sikkerhetsklarering?	Autorisasjon?	Tjenstlig behov?	
Ja	Ja	Ja	Dedikert
Ja	Ja	Nei	Fellesnivå
Ja	Nei	Nei	Partisjonert
Nei	Nei	Nei	Flernivå

For dedikerte informasjonssystemer betyr dette at alle brukerne har tjenstlig behov for all informasjonen som finnes på systemet. Dersom det er usikkert om alle brukerne har samme tjenstlige behov, bør man velge en annen operasjonsmåte. På fellesnivå operasjonsmåte har alle brukere samme minimum sikkerhetsklarering og autorisasjon, men ikke samme tjenstlige behov for all informasjonen. For informasjonssystemer med partisjonert operasjonsmåte har alle brukerne samme minimum sikkerhetsklarering, men ikke samme autorisasjon eller tjenstlig behov. Dersom man har et informasjonssystem hvor man har brukere med ulik sikkerhetsklarering, autorisasjon og tjenstlig behov faller dette inn under flernivå operasjonsmåte.

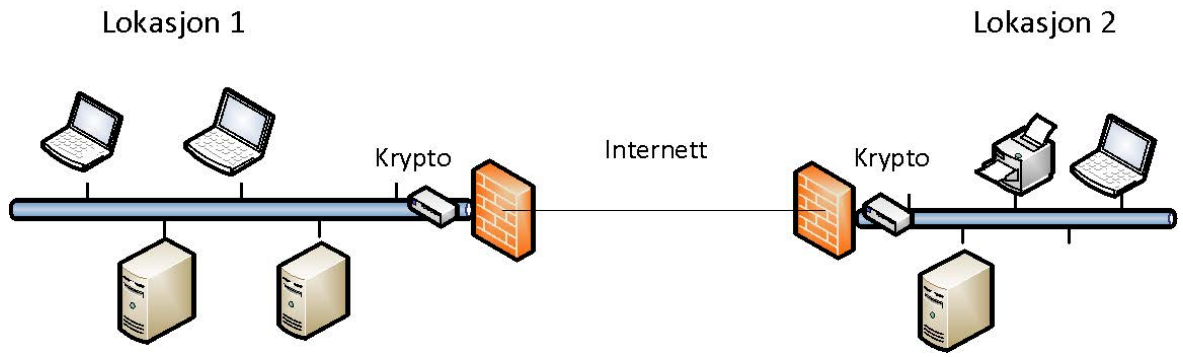
Hvilken operasjonsmåte informasjonssystemet faller inn under har betydning for hvem som er godkjenningsmyndighet og for hvilke krav NSM stiller i sine veiledere til sikring av informasjonssystemet.

9 Om informasjonssystemet

Når man setter i gang med planleggingen av et gradert informasjonssystem må man definere informasjonssystemets hensikt og bruksområde.

Man må også så tidlig som mulig danne seg et bilde av informasjonssystemets fysiske og virtuelle omfang, da dette kan få betydning for det senere sikkerhetsarbeidet. Beskrivelsen av omfang bør inkludere sentralutrustning, type og antall klienter, nettverksinfrastruktur, antall brukere og brukersteder samt eventuelt behov for utvekslingsgrensesnitt mot andre informasjonssystemer (fysisk og virtuelt).

Det bør utarbeides en overordnet systemskisse slik at man kan danne seg et bilde av løsningen. En enkel systemskisse kan for eksempel se slik ut:



10 Geografisk og fysisk plassering

Når man planlegger et gradert informasjonssystem er det viktig at man tenker på hvor dette skal benyttes. Informasjonssystemets geografiske lokasjon er omgivelsene hvor informasjonssystemet er plassert, som for eksempel hvor i landet (evt. utlandet) informasjonssystemet skal benyttes og en overordnet beskrivelse av omkringliggende områder. Informasjonssystemets plassering i forhold til omgivelsene og installasjoner i nærheten vil innvirke på sikringskravene, både med tanke på fysisk sikring og TEMPEST.

Med fysisk plassering menes det informasjonssystemets spesifikke fysiske plassering og i hva slags type soner (kontrollert, beskyttet, sperret område[2]) man forutsetter å plassere forskjellige deler av informasjonssystemet, som servere, nettverksinfrastruktur, kabelstrekk og klienter. Andre spesielle forhold ved den fysiske sikringen bør også komme fram.

Dersom en virksomhet skal oppbevare eller behandle gradert informasjon skal virksomhetens områder deles inn i ulike fysiske områder. De ulike områdene har egne krav til sikring ut i fra graderingen på informasjonen som behandles eller oppbevares der. For eksempel er det strengere krav til sikring av sperret område for HEMMELIG informasjon enn for BEGRENSET. Planleggingsfasen må avklare i hvilke typer område det vil være aktuelt å benytte informasjonssystemet.

11 Elektromagnetisk stråling (TEMPEST)

Informasjonssystemer som skal behandle gradert informasjon på nivå KONFIDENSIELT eller høyere i Norge, eller BEGRENSET eller høyere i utlandet, skal beskyttes mot at uvedkommende kan få tilgang til informasjonen i systemet gjennom kompromitterende elektromagnetisk stråling (TEMPEST).

I alle tilfeller der det er krav om beskyttelse mot TEMPEST skal det utarbeides en TEMPEST risikovurdering. TEMPEST risikovurderingen skal dokumentere trusler, sårbarheter og verdier med fokus på TEMPEST, samt beskrive nødvendige TEMPEST tiltak.

Et sikkerhetskonsept skal inneholde resultatet av TEMPEST risikovurderingen. Dette vil typisk være minste inspiserbare område og eventuelt hvilke TEMPEST-tiltak som må innføres for informasjonssystemet på overordnet nivå. Vær oppmerksom på at det er ulike krav til TEMPEST-sikring av informasjonssystemer i Norge og i utlandet. Informasjonssystemets geografiske plassering har derfor stor betydning. Det anbefales at man gjør TEMPEST risikovurderingen så tidlig som mulig i prosessen, da det kan medføre uforutsette ekstrakostnader om man gjør det etter at man kjøpt inn utstyr.

NSM har en veiledning i TEMPEST-sikring av IKT-systemer. Denne er gradert BEGRENSET og er tilgjengelig på forespørsel.

[2] Veiledning i fysisk sikring mot ulovlig inntrengning

12 Kommunikasjon og sammenkoblinger

Dersom informasjonssystemet skal ha forbindelse utenfor kontrollert område skal kommunikasjonen krypteres, slik at ikke uvedkommende kan få tilgang til informasjonen som sendes. For å sikre norsk sikkerhetsgradert informasjon skal det kun benyttes kryptoutstyr forhåndsgodkjent av NSM. Dersom informasjonssystemet også skal behandle NATO-gradert informasjon på nivå NATO SECRET eller høyere må kryptoutstyret være forhåndsgodkjent for dette av NATO.

Dersom et informasjonssystem skal kobles sammen med en annen virksomhet sitt informasjonssystem skal det foreligge en sammenkoblingsavtale som avklarer roller og ansvar mellom virksomhetene. Hvis flere enn to informasjonssystemer skal kobles sammen skal dette skje via et eget informasjonssystem dedikert til dette formålet. Dersom to eller flere informasjonssystemer skal sammenkobles må muligheten for dette fremkomme i begge systemenes sikkerhetskonsept. Dette ivaretar at systemene innehar beskyttelsesmekanismer som håndterer påvirkningen en sammenkobling vil ha.

I planleggingsfasen må forbindelser utenfor kontrollert område og sammenkoblinger med andre informasjonssystemer kartlegges, slik at man kan ta høyde for disse når man senere skal identifisere sikkerhetskravene som gjelder for løsningen.

13 Systemtekniske aspekter

Et informasjonssystems systemtekniske aspekter er de ulike tekniske egenskapene som til sammen utgjør systemets helhet. Det er viktig at man i løpet av planleggingsfasen i utviklingsløpet får avklart fakta om informasjonssystemet slik at alle parter kan gjøre seg kjent med overordnete rammer og sikkerhetskrav for informasjonssystemet som skal utvikles. Elementer som bør beskrives er teknologivalg, sentral sikkerhetsfunksjonalitet og hvordan denne gjenbrukes samt beskrivelse av systemets design, herunder overordnet arkitektur og konfigurasjon. Videre bør sentrale forutsetninger og valg som er avgjørende for vedlikehold og drift av informasjonssystemet, samt deteksjon og håndtering av hendelser beskrives.

De vurderingene man har gjort tidligere i konseptet vil ligge til grunn for de systemtekniske valgene som gjøres. Det er derfor viktig å være så presis som mulig, spesielt når det gjelder bruksområde, miljø og verdivurdering, for å ikke bli tvunget til å forholde seg til unødig strenge krav. Det er ikke forventet at man på dette tidspunktet skal gjøre rede for hvert enkelt krav man skal innføre, men på overordnet nivå beskrive systemtekniske forutsetninger og valg som vil gi føringer for hvilke krav som vil settes. Kravene som utledes vil baseres på NSMs generelle teknologiveiledere (G-veiledere), teknologispesifikke veiledere eller anerkjente beste praksis på de områdene hvor NSM ikke har egne veiledere. Man bør på dette tidspunktet gjøre en vurdering av hvilket rammeverk som skal ligge til grunn for drift og vedlikehold av informasjonssystemet, som ITIL eller liknende.

13.1 Sikkerhetsevaluering og sertifisering

Det er krav til tillit til sentral sikkerhetsfunksjonalitet i et gradert informasjonssystem. Slik funksjonalitet kan for eksempel være del av operativsystem, brannmur eller annen nettverksinfrastruktur. Tillit etableres gjennom en formell evaluering som også kan resultere i en sertifisering av et produkt. Det er derfor en fordel å velge produkter som allerede innehar en sertifisering, for eksempel Common Criteria-sertifisering eller tilsvarende.

Kryptoutstyr og filtre, dioder eller liknende som benyttes for separasjon mellom graderingsnivåer eller sikkerhetsdomener skal evalueres og sertifiseres. NSM er sertifiseringsmyndighet. I tillegg skal følgende evalueres og sertifiseres, såfremt NSM ikke bestemmer noe annet:

- Fellesnivå informasjonssystem for HEMMELIG eller høyere
- Partisjonerte informasjonssystemer
- Flernivå informasjonssystemer

Målet med en evaluering er å etablere et rett tillitsnivå til grunnleggende sikkerhetsfunksjonalitet. Dette vil typisk være sikkerhets- og tilgangskontrollmekanismer i operativsystemet og tilsvarende i eventuelle applikasjoner som ikke gjenbruker sikkerhetsmekanismene i operativsystemet.

Krav til evaluering og sertifisering vil avhenge av en helhetlig vurdering av valgt løsning med utgangspunkt i sikkerhetskonseptet. Derfor er det viktig å kontakte NSM så tidlig som mulig etter at man er ferdig med utkast til sikkerhetskonsept. Dersom man kommer tidlig i gang med dette arbeidet unngår man unødige forsinkelser i godkjenningsprosessen.

14 Risikovurdering

Når man har klart for seg grunnlaget, eller sikkerhetskonseptet, for informasjonssystemet skal det gjennomføres en foreløpig risikovurdering på bakgrunn av resultatet av verdivurderingen, en trusselvurdering og eventuelle sårbarheter som kan identifiseres på bakgrunn av sikkerhetskonseptet.

I en senere fase av utviklingsarbeidet kan denne risikovurderingen, og da spesielt trusselvurderingen, legges til grunn for å vurdere om det er behov for å innføre ytterligere tiltak ut over det som er minimumskravene som stilles i forskrift om informasjonssikkerhet og NSMs veiledninger.

15 Godkjenningsmyndighet

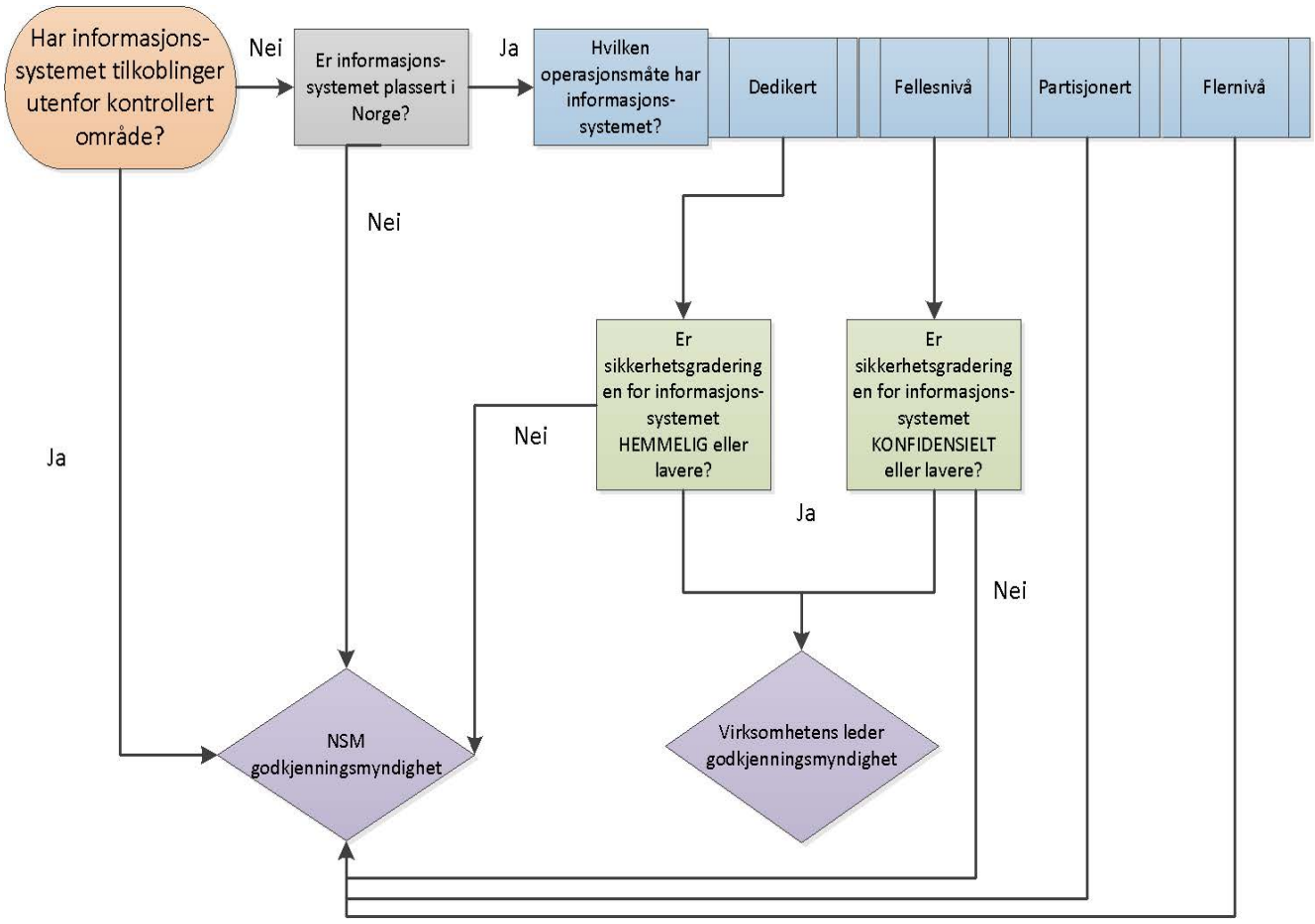
Godkjenningsmyndigheten skal saksbehandle søknader om sikkerhetsgodkjenning eller midlertidig brukstillatelse og skal til en hver tid ha oversikt over systemer som er sikkerhetsgodkjent eller har midlertidig brukstillatelse innenfor deres ansvarsområde. Godkjenningsmyndigheten skal også gi råd og veiledning i forbindelse med gjennomføring av sikkerhetsgodkjenning.

Godkjenningsmyndigheten setter krav til en prosess for gjennomføring av sikkerhetsgodkjenning. Denne skal dokumenteres i en godkjenningsstrategi.

Godkjenningsmyndigheten skal gjennomgå relevant sikkerhetsdokumentasjon utarbeidet i forbindelse med utviklingen av informasjonssystemet. Dette kan for eksempel være sikkerhetskonsept, kravspesifikasjon for sikkerhet, samsvarserklæringer, evalueringsrapporter, bruker- og driftsinstrukser og lignende.

Operasjonsmåte, gradering, sammenkoblinger og geografisk plassering avgjør om det er NSM eller virksomheten selv som er godkjenningsmyndighet. I tilfeller hvor NSM er godkjenningsmyndighet avtales det i godkjenningsstrategien hvilken dokumentasjon som skal fremsendes sammen med søknaden. Hvis det er virksomheten selv som er godkjenningsmyndighet skal rapport om sikkerhetsgodkjenning av informasjonssystemet sendes til NSM, som skal ha et sentralt register over alle graderte informasjonssystemer i Norge.

Flytskjemaet under viser hvordan man kommer frem til hvem som er godkjenningsmyndighet for et informasjonssystem.



16 Godkjenningsstrategi

Godkjenningsstrategien beskriver godkjenningsprosessen for det enkelte informasjonssystem. Den er en avtale mellom aktørene i godkjenningsarbeidet og godkjenningsmyndigheten som beskriver ansvar, roller og leveranser. Selv om det er virksomheten selv som er godkjenningsmyndighet kan det være hensiktsmessig å ha en godkjenningsstrategi, særlig dersom det er mange enheter involvert i arbeidet. En godkjenning gjelder normalt for tre år, mens en midlertidig brukstillatelse gis for maksimalt seks måneder.

16.1 Ansvar og aktører

Ansvar som for eksempel utviklingsansvarlig, driftsansvarlig, brukerstedstedsansvarlig, godkjenningsmyndighet og eventuelt andre som skal delta i godkjenningsarbeidet må defineres i godkjenningsstrategien. Her skal hver aktørs plikter og roller, samt hvem som innehar disse rollene beskrives. Utviklingsansvarlig, driftsansvarlig og brukerstedsansvarlig er nærmere beskrevet i kapittel 3 i denne veilederen. En aktør kan inneha flere roller, eller rollene kan deles opp på en annen måte enn det som er beskrevet i denne veilederen ut i fra hva som er hensiktsmessig i det enkelte tilfelle.

16.2 Sikkerhetsdokumentasjon

I godkjenningsstrategien skal det avtales hvilke dokumenter som skal utarbeides og hvilke aktører som er ansvarlig det enkelte dokument. Formålet med sikkerhetsdokumentasjonen er å hjelpe til med

å sikre og opprettholde informasjonssystemets sikre tilstand. Ansvar for dokumentasjonen som skal utarbeides kan med fordel deles opp på følgende måte:

Utviklingsansvarlig	Driftsansvarlig	Brukerstedsansvarlig
Sikkerhetskonsept Godkjenningsstrategi For referanseløsningen: - overordnet systemdesign - sikkerhetskrav - sikkerhetstiltak - testplaner - sårbarhetsvurdering - evalueringsrapporter Krav til sikker drift, vedlikehold, deteksjon og hendelseshåndtering samt sikker bruk	Instrukser og rutiner for sikker drift, vedlikehold, deteksjon og gjenoppretting, herunder: - administratorroller - installasjon og oppsett - brukeradministrasjon - tilgangskontroll - konfigurasjon (SW/HW) - konfigurasjonskontroll - verifikasjon - overvåkning - backup og reservedrift - vedlikehold og avhending - skadevarebeskyttelse Lokal sikkerhetsdokumentasjon - styring og kontroll - organisering - personellsikkerhet - fysisk sikring - TEMPEST - kabelkart Test- og verifikasjonsplaner Risikovurdering basert på avvik fra krav	Instrukser og rutiner for sikker bruk Lokal sikkerhetsdokumentasjon - styring og kontroll - organisering - personellsikkerhet - fysisk sikring - TEMPEST - kabelkart Test- og verifikasjonsplaner Risikovurdering basert på avvik fra krav

16.3 Evaluering og sertifisering

Dersom det er krav om evaluering og sertifisering av hele eller deler av informasjonssystemet skal prosess for dette avtales i godkjenningsstrategien. Det er derfor viktig å ta kontakt med NSM så tidlig som mulig i planleggingsfasen, slik at en eventuell evaluering ikke forsinker den videre prosessen.

16.4 Gjennomføringsplan

En gjennomføringsplan er en beskrivelse av hvordan selve godkjenningsarbeidet skal foregå. Denne skal beskrive leveranser i forbindelse med godkjenningsprosessen, både til virksomheten og NSM helt frem mot endelig godkjenning. Gjennomføringsplanen kan skrives som en del av godkjenningsstrategien, eller være et vedlegg til denne.

16.5 Inndeling i elementer

En sikkerhetsgodkjenning er en avgjørelse om at et informasjonssystem i en virksomhet tillates brukt til behandling, lagring eller transport av sikkerhetsgradert informasjon. For å forenkle godkjenningsprosessen og legge til rette for gjenbruk kan informasjonssystemet deles inn i elementer som kan godkjennes hver for seg[3]. På overordnet nivå kan et informasjonssystem deles inn i

[3] Forskrift om informasjonssikkerhet § 5-34. I forskriften omtales «elementer» som «moduler».

referanseløsning, driftsløsning og brukersted. Dette avtales i godkjenningsstrategien. Her kan det også avtales inndeling av referanseløsningen i ytterligere tekniske moduler om det er hensiktsmessig, samt hvordan disse skal godkjennes.

16.5.1 Referanseløsning

Referanseløsningen til et informasjonssystem er den systemtekniske konfigurasjonen, arkitekturen og beskrivelsene av prosessene for informasjonssystemet. Referanseløsningen tas frem av utviklingsansvarlig og det er normalt utviklingsansvarlig som har ansvaret for forvaltningen av denne, det vil si at endringer og sikkerhetsoppdateringer integreres i referanseløsningen. Referanseløsningen skal ivareta hovedmålet om sikker plattform som innebærer at det skal dokumenteres en sikker tilstand gjennom en helhetlig og enhetlig infrastruktur og nødvendig sikkerhetsfunksjonalitet. Referanseløsningen kan sees på som et mønster med overordnede krav til hvordan informasjonssystemet skal driftes og brukes. Referanseløsningen kan godkjennes for seg med en referansegodkjenning.

For en referanseløsning må det først utarbeides et sikkerhetskonsept. På bakgrunn av dette må nødvendige krav til sikring utledes. Det må her tas utgangspunkt i NSMs veiledere på området. Kravene skal ikke bare dekke de systemtekniske kravene i referanseløsningen, men også krav til sikker drift, vedlikehold, deteksjon og hendelseshåndtering, samt sikker bruk. Utviklingsansvarlig må så utlede og beskrive sikkerhetstiltakene som møter kravene til referanseløsningen. Driftsansvarlig og brukerstedsansvarlig utleder og beskriver sikkerhetstiltak innen deres ansvarsområder. Utviklingsansvarlig utarbeider også planer for test og verifikasjon av systemtekniske sikkerhetstiltak som gjennomføres av ansvarlige innen de forskjellige områdene. Alt dette må dokumenteres.

Referanseløsningen kan videre deles inn i tekniske moduler. Dette kan være definerte mengder teknologi som sikkerhetsmessig kan betraktes som en enhet. Det kan i godkjenningsstrategien avtales at slike tekniske moduler kan godkjennes hver for seg.

16.5.2 Driftsløsning

Driftsløsningen til et informasjonssystem er implementasjonen av referanseløsningen hos den som er ansvarlig for drift av informasjonssystemet og således leverer tjenesten til brukerstedene. Driftsløsningen innbefatter informasjonssystemets sentralutrustning som servere, nettverkskomponenter og øvrig infrastruktur, i tillegg til de nødvendige prosedyrene og rutinene som skal ivareta sikker drift og vedlikehold av informasjonssystemet. Driftsløsningen inkluderer også prosedyrene og rutinene som sikrer at konfigurasjonen regelmessig kontrolleres opp mot den sikre tilstanden som beskrevet i referanseløsningen. Driftsløsningen skal ivareta tilstrekkelig deteksjon av uønskede hendelser gjennom verktøy og rutiner. Driftsansvarlig er også ansvarlig for å ha prosedyrer og rutiner for å håndtere avvik og hendelser slik at informasjonssystemets sikre tilstand til en hver tid ivaretas eller raskt kan gjenopprettes.

For at en driftsløsning skal kunne fremlegges for godkjenning må også de lokale sikringstiltakene hos driftsansvarlig være implementert, dokumentert og verifisert. Det vil si at det må være en sikkerhetsorganisasjon med tilstrekkelig kompetanse og ressurser til å ivareta sikkerheten i driftsløsningen og nødvendige fysiske og personellmessige sikringstiltak må være på plass. Det kan også være krav om tiltak innen krypto og TEMPEST.

Det skal være etablerte rutiner for gjennomføring av sikkerhetsrevisjon av driftsløsningen minimum årlig.

16.5.3 Brukersted

Brukerstedet er den eller de fysiske lokasjonene hvor informasjonssystemet skal benyttes til å behandle gradert informasjon.

For at brukerstedet skal kunne få brukerstedsgodkjenning må de lokale sikringstiltakene være implementert, dokumentert og verifisert. Det vil si at det må være en sikkerhetsorganisasjon med

tilstrekkelig kompetanse og ressurser til å ivareta sikkerheten og nødvendige fysiske og personellmessige sikringstiltak, samt rutiner og prosedyrer på plass. Det kan også være krav om tiltak innen krypto og TEMPEST.

Alle brukere av informasjonssystemet må ha tilstrekkelig opplæring og være kjent med kravene til sikker bruk og det må regelmessig gjennomføres tiltak for bevisstgjøring av brukerne.

Det skal være etablerte rutiner for gjennomføring av sikkerhetsrevisjon av sikringstiltak på brukerstedet minimum årlig.