Försvarsmakten
107 85 STOCKHOLM

Datum 2006-06-21
Dnr 32-2005-0551

FÖRSVARSMAKTENS STYRNING AV INFORMATIONSSÄKERHETSARBETET

Riksrevisionen har som ett led i den årliga revisionen av Försvarsmakten granskat myndighetens process för styrning av informationssäkerhetsarbetet.

Granskningen har genomförts med stöd av konsult från företaget Transcendent Group, och har resulterat i nedanstående iakttagelser.

Riksrevisionen önskar information senast 2006-08-18 med anledning av våra iakttagelser i denna rapport.

1. Inledning

I takt med att inslagen av elektronisk förvaltning ökar hos de flesta statliga myndigheter och allt större krav ställs på att e-tjänsterna är säkra, inte minst för att medborgare och företagare ska ha förtroende för dessa tjänster, ökar också kraven på en god informationssäkerhet. Med denna utveckling följer att myndigheterna behöver se över och vid behov förstärka sitt informationssäkerhetsarbete för att bringa detta i paritet med den förändrade riskbilden som följer bl.a. med den elektroniska förvaltningen.

I denna granskning har tyngdpunkten legat på den interna styrningen och kontrollen för att säkerställa skyddet av Försvarsmaktens IT-relaterade informationstillgångar. Avgränsningen innebär att faktiskt uppnådd säkerhet i enskilda system inte har granskats.

Den huvudsakliga normkällan för de bedömningar som gjorts vid granskningen har varit standarden Ledningssystem för informationssäkerhet (SS 627799 och SS-ISO/IEC 17799).

De normer som använts för att bedöma och värdera iakttagelserna från granskningen, har i rapporten strukturerats efter kontrollkomponenterna i intern styrning och kontroll i enlighet med COSO-modellen[1]. Enligt COSO-modellen omfattar intern kontroll följande delar:

- kontrollmiljö
- riskanalys
- kontrollfunktioner
- information och utbildning

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO) har beskrivit den interna styrningens och kontrollens olika beståndsdelar och deras samband i den s.k. COSO-modellen.

- uppföljning och utvärdering

En beskrivning av bedömningskriterierna för respektive komponent inleder respektive avsnitt nedan.

2. Försvarsmakten och informationssäkerhet

2.1 Allmänt

Försvarsmaktens verksamhet har ett högt beroende av fungerande informationssäkerhetsrutiner, då verksamheten omfattar hantering av material som omfattas av såväl sekretess, som krav på hög tillgänglighet.

Riksrevisionens samlade bedömning är att Försvarsmakten på en övergripande nivå har ett samlat och strukturerat förhållningssätt till informationssäkerhetsfrågor. Överbefälhavaren har den 1 december 2001 fattat beslut om att införa en ”Försvarsmaktsstandard för ett integrerat verksamhetsledningssystem”. Den 1 december 2003 beslutade överbefälhavaren att 2003 års utgåva av Försvarsmaktsstandard för integrerat verksamhetsledningssystem (FMS VHL2003) skall tillämpas. Denna standard omfattar bl.a. en informationssäkerhetsdimension. Den 13 juni 2005 beslutades att informationssäkerhetsdimensionen skall utgå från standarden ISO/IEC 17799, och att specificering av införandet framgår av dokumentet ”Uttalande om tillämplighet - ISO/IEC 17799 (SS 62 77 99) för Försvarsmakten”, med tillämpning från den 1 juli 2005.

Militära underrättelse- och säkerhetstjänsten leder och samordnar informationssäkerhetsarbetet vid Försvarsmakten, medan det praktiska ansvaret för informationssäkerhet i system m.m. är delegerat till produkt- och verksamhetsansvariga i organisationen.

Nedan redovisas kortfattat vissa av de kriterier som legat till grund för våra bedömningar. I bilaga till rapporten återfinns en mera detaljerad genomgång från Transcendent Group, avseende 28 förbättringsområden som noterats i samband med granskningen.

2.2 Kontrollmiljö

Bedömningskriterier

Kontrollmiljön är en del av myndighetskulturen och skapas av myndighetens chefer. En god kontrollmiljö kännetecknas bl.a. av:

- Ett tydligt visat engagemang från ledningen.
- En från ledningen kommunicerad syn på betydelsen av intern styrning och kontroll av informationssäkerheten, vilket kan ske i en informationssäkerhetspolicy.
- Att ledningen skapat tillräckliga resurser för arbetet med informationssäkerheten.

- Inrättandet av tydliga funktioner – periodiska genomgångar, säkerhetsansvarig, rapporteringsrutiner m.m. – för att kontrollera om organisationen av informationssäkerheten och införda säkerhetsåtgärder fungerar enligt ledningens intentioner och beslut.

Iakttagelser och bedömningar från granskningen

Som konstaterats ovan har en informationssäkerhetsdimension, baserad på standarden ISO/IEC 17799 införts i Försvarsmaktens verksamhetsledningssystem. Överbefälhavaren har den 5 april 2005 beslutat om en övergripande informationssäkerhetspolicy för Försvarsmakten. Försvarsmakten tillhandahåller vidare ett omfattande internt styrnings- och referensmaterial, som specificerar olika aspekter inom informationssäkerhetsområdet. Därutöver finns även ett antal externa regelverk, såsom Säkerhetsskyddslagen (1996:627) som i hög grad är tillämpliga i verksamheten.

Ägarrollerna för Försvarsmaktens informationssystem kan kortfattat beskrivas i tre roller:

- *Produktägare:* den enhetschef i Högkvarteret eller den chef för en organisationsenhet som har det huvudsakliga ansvaret för ett IT-system.

- *Driftägare:* den chef för en organisationsenhet som ansvarar för driften av IT-system.

- *Systemägare:* den chef för en organisationsenhet som ansvarar för den del av ett IT-system som skall användas i den egna verksamheten.

På organisatorisk enhetsnivå finns normalt sett en säkerhetschef, IT-säkerhetschef samt signalskyddschef. Något formellt krav på att en lokal *informationssäkerhetschef* skall finnas är inte definierat. I praktiken anses dock informationssäkerhetsansvaret åvila respektive produkt- och systemägare, medan MUST (Militära underrättelse- och säkerhetstjänsten) ansvarar för att leda och samordna informationssäkerhetsarbetet på en övergripande nivå. Det kan dock noteras att MUST för närvarande även har en stödjande funktion för informationssäkerhetsarbetet vid utlandsstyrkan, vilket kan vara problematiskt då man i detta fall till viss del riskerar att utöva kontroll över egen verksamhet.

I övrigt ansvarar MUST således för myndighetsövergripande föreskrifter, interna bestämmelser samt handböcker inom området, medan chefen för en organisationsenhet skall fastställa *lokala* riktlinjer för säkerhetsarbetet i en IT-säkerhetsplan. I dessa riktlinjer realiseras i princip *hur* enheten skall uppnå de mål och krav som ställts i centrala styrdokument. Dessa lokala riktlinjer skall lämpligen avspegla de mål och inriktningar för verksamhetsledningssystemet (och därmed informationssäkerhetsdimensionen) som ledningen för en organisationsenhet skall fastställa enligt FMS VHL 2003.

Riksrevisionen har vid granskningen fått en blandad bild av hur ovanstående modell fungerar i praktiken. Detta rör områden som, åtminstone indirekt kan ha effekt på möjligheten att uppfylla de övergripande krav som ställs på informationstillgångarnas *sekretess*, *tillgänglighet*, *riktighet* och *spårbarhet*. Riksrevisionens bild är att det från förbandens sida i vissa fall upplevs finnas begränsade möjligheter att realisera sina önskemål, avseende exempelvis hantering av supportärenden samt vissa investeringsbehov. Motsvarande synpunkter har också noterats rörande möjligheten att från lokal nivå medverka som remissinstans i större utvecklingsprojekt mm. Det bör noteras att centrala instanser vid Försvarsmakten anser att denna möjlighet ges förbanden i tillräcklig utsträckning, men Riksrevisionen anser det ändå värt att notera de synpunkter som framkommit. Detta då eventuella brister i verksamhetsförankring i utvecklings- och driftsprocesser, kan leda till att eftersträvade effektivitetsmål inte uppnås.

Granskningen indikerar också att det under en övergångsperiod kan uppfattas, eller har uppfattats, som osäkert vilken status informationssäkerhetsdimensionen, och FMS VHL 2003, har i förhållande till tidigare gällande regelverk som fastställts av KRI LED. Försvarsmakten anser själva att detta problem i huvudsak lösts under 2005.

Riksrevisionens sammantagna bild av kontrollmiljön rörande Försvarsmaktens informationssäkerhetsarbete är att det finns tydliga intentioner och direktiv från ledningen inom området, vilket är en grundläggande förutsättning för ett effektivt informationssäkerhetsarbete. En risk är dock den, jämfört med många andra organisationer, långtgående delegeringen av det operativa säkerhetsansvaret, med den därpå följande friheten att utforma lokala regelverk inom området. Detta ställer särskilda krav på såväl tydlighet i centrala inriktningsbeslut och regelverk, som effektiva uppföljande och kontrollerande åtgärder, för att myndighetsledningen skall kunna säkerställa att dess ansvar enligt bl.a. §6-7 Verksförordningen (1995:1322) är uppfyllt. Som motvikt till detta resonemang kan givetvis anföras att ett tydligt uttalat ansvar för lokala befattningshavare ökar sannolikheten att frågorna på lokal nivå åsätts relevant prioritet ute i verksamheten. Riksrevisionen kan också konstatera att det inom organisationen finns olika uppfattningar om i vilken omfattning verksamhetsföreträdare i praktiken kan påverka exempelvis utvecklings- och investeringsprocesser.

2.3 Riskanalys

Bedömningskriterier

Riskhantering är aktiviteter på ledningsnivå som bör omfatta en process för systematisk riskanalys - innebärande att de utförs med hjälp av beslutade systematiska[2] och dokumenterade metoder. Denna process omfattar analyser och bedömningar av väsentliga hot, risker och konsekvenser.

[2] Exempel på riskanalysmetoder är SBA Scenario, RiscPac, CRAMM, RA, ISAP, ISF Sprint och Proteus.

Vidare bör det finnas en åtgärdsplan som förtecknar beslutade åtgärder för att möta de risker som framkommit i analysen t.ex. avbrottsplanering, förstärkning av skyddsåtgärder, skadefinansiering och eventuellt försäkringsskydd. Planen bör beskriva när åtgärderna ska vara genomförda och vilka som ansvarar för deras genomförande. Genomförandet bör följas upp.

Som underlag för analysen behövs identifiering[3] av de skyddsvärda informationstillgångarna. De bör dokumenteras i en överblickbar förteckning. Åtminstone de tillgångar som är strategiska för verksamheten bör åsättas en beslutad säkerhetsnivå[4] – klassning - med hänsyn till verksamhetens krav på tillgänglighet, riktighet och sekretess så att en prioritering av åtgärder kan göras.

Riskanalysen bör årligen och däremellan vid behov prövas.

Iakttagelser och bedömningar från granskningen

Enligt säkerhetsskyddsförordningen (1996:633) skall en myndighet undersöka vilka uppgifter i dess verksamhet som skall hållas hemliga med hänsyn till rikets säkerhet. Vid Försvarsmakten görs detta genom att *produktägaren* i ett första steg, baserat på en informationsklassning, bedömer om ett system är avsett att behandla hemliga uppgifter. Uppgifterna placeras utifrån denna bedömning i en informationssäkerhetsklass, vilket följer av Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd. Även vad gäller de övriga informationssäkerhetsmålen (tillgänglighet, riktighet och spårbarhet) så ansvarar produktägaren för de krav som ska ställas. Detta ställningstagande dokumenteras för respektive produkt och ligger sedan till grund för det fortsatta auktorisations- och ackrediteringsarbetet av produkten/systemet.

De förbandsbesök som gjorts vid granskningen indikerar att riskanalyser upprättats lokalt och omprövas med viss regelbundenhet. Riksrevisionen har dock vid granskningen noterat att arbetet med riskanalyser inte följer något standardiserat, internt regelverk och därför kan upprättas utifrån olika metoder. Riksrevisionen har inte heller identifierat något krav på att enheterna regelbundet skall inrapportera resultatet av sina analyser till central instans, mer än i samband med den lokala ackrediteringen av en applikation/tjänst. Riksrevisionen anser att detta är ett område som bör utvecklas. Detta då nuvarande förfarande, enligt Riksrevisionens bedömning, kan medföra risk att såväl central sammanställning och analys av den övergripande riskbilden, som ett effektivt informationsutbyte mellan organisatoriska enheter kan försvåras.

I detta sammanhang kan det också vara värt att beakta om den pågående konsolideringen av IT-miljön vid Försvarsmakten, där antalet lokala variationer av programvaror kommer att minska kraftigt, bör föranleda en annan syn på behovet av riskbedömningar på övergripande nivå. Riksrevisionen anser att det i större utsträckning borde vara aktuellt tillämpa

[3] Identifieringen bör omfatta :vilka de är, vilka som är ägare/har ansvar för dem, var de finns samt vilka kopplingar till andra tillgångar respektive tillgång kräver när den används.

[4] Ett sätt att prioritera är att utifrån ledningens syn på konsekvenser av brister ange klasser i olika nivåer (t.ex. Mycket kritiskt, Viktigt, Mindre viktigt).

en metod med återkommande, sammanställd analys som beaktar och involverar samtliga intressenter, såväl lokala som centrala, i processer där flera intressenter, system eller tjänster berörs. Detta för att säkerställa att alla relevanta riskområden omhändertas i analysprocessen, och därigenom kan mötas med lämpliga skyddsåtgärder.

Vid löpande granskning av Försvarsmaktens verksamhet har några exempel iakttagits som kan exemplifiera ovan nämnt behov. I samband med såväl årsredovisningen 2004, som delårsrapporten 2005 avlämnade Riksrevisionen revisionsberättelse med invändning till Försvarsmakten. Detta pga. att revisionen bedömde att det redovisade värdet på Försvarsmaktens beredskapstillgångar, uppgående till ca 90 miljarder kr inte kunde verifieras på ett tillfredsställande sätt. Som noterats i revisionsrapport över granskning av Försvarsmaktens årsredovisning 2005 (daterad 2006-03-24), har Försvarsmakten därefter identifierat att värdet av lagertillgångar uppgående till ca 2,4 miljarder kr, såväl tidigare år, som i 2005 års delårsrapport, saknades i den finansiella redovisningen. Detta pga. att indata i aktuella försystem inte har var komplett, vilket fick till följd att samtliga informationsmängder inte fördes över till den finansiella redovisningen. I samma rapport noteras även att brister kvarstår vad gäller fullständighet och riktighet i grund- och förvaltningsdata för andra informationsmängder i berörd process. Detta bedöms kunna få konsekvenser för såväl den finansiella redovisningen som för lokala enheters möjlighet att utföra sitt arbete på ett kostnadseffektivt sätt. En sannolik orsak till dessa problem kan vara att den aktuella applikationens funktionalitet inte konstruerats utifrån samtliga de funktioner applikationen idag förväntas fyllas, möjligen pga. att kravbilden förändrats sedan applikationen infördes. Riksrevisionen bedömer därför att nuvarande systemstöd inte är adekvat för att på ett tillförlitligt och effektivt sätt kunna hantera redovisningen av Försvarsmaktens beredskapstillgångar. Detta kan ses som exempel på risker som uppstår i processer som berör flera applikationer eller flera intressenter, och som enligt Riksrevisionens bedömning ställer särskilda krav på såväl riskanalys, som kontinuerlig uppföljning och kontroll av riktighet i information och informationsöverföring.

Riksrevisionen kan vidare konstatera att Försvarsmakten på flera områden är inne i en omfattande förändringsprocess som ställer krav på en regelbunden bedömning av om såväl informationssäkerhetskrav, som verksamhetskrav kan uppnås med nuvarande systemstöd och regelverk. Exempel som särskilt bör beaktas är risker förknippade den pågående omstruktureringen av Försvarsmakten, ökat deltagande i internationella insatser och övningar samt aktiviteter som inte tidigare varit vanligt förekommande i Försvarsmaktens verksamhet, exempelvis försäljningen av JAS-plan till andra nationer.

Sammantaget bedömer Riksrevisionen att en tydligare central styrning, samordning och uppföljning av riskanalysarbetet skulle underlätta myndighetsledningens bedömning av den totala riskbilden för myndigheten. Riksrevisionen vill vidare särskilt påtala behovet av att riskanalysarbetet fokuseras på de processer där information och informationstillgångar skall användas, och inte blir alltför systeminriktat. Detta för att säkerställa att alla relevanta riskområden omhändertas i analysprocessen, och därigenom kan mötas med lämpliga skyddsåtgärder. Som konstaterats ovan, har under

löpande granskning av Försvarsmakten iakttagits områden där Riksrevisionen anser att nuvarande systemstöd inte stödjer berörda verksamhetsprocesser på ett tillfredsställande sätt.

Vad gäller klassificering av information bedömer Riksrevisionen dock att Försvarsmakten har ett ramverk som ger förutsättningar för att en god säkerhetsnivå skall kunna upprätthållas. Riksrevisionen bedömer slutligen att pågående förändringar av Försvarsmaktens organisation och verksamhetsinriktning ställer särskilda krav på en fortsatt utveckling av analys och riskhantering.

2.4 Ledningens kontrollfunktioner

Bedömningskriterier

Kontrollfunktioner är i detta sammanhang dels åtgärder som ledningen utformat för att förebygga, upptäcka och åtgärda brister i informationssäkerheten, dels enskilda säkerhetsåtgärder som syftar till att skydda informationstillgångar eller skydda själva säkerhetsåtgärden. Kontrollfunktionerna utgör sammantaget myndighetens ledningssystem för informationssäkerhet (LIS).

Det bör finnas en till all personal kommunicerad skriftlig beskrivning av roller[5] i informationssäkerhetsarbetet och hur ansvar och befogenheter för myndighetens informationssäkerhet fördelats på dessa. Vidare bör alla medarbetares eget ansvar framgå.

LIS bör om inte särskilda skäl[6] finns omfatta följande komponenter[7]:

- Informationssäkerhetspolicy
- Process för incidentrapportering inkl. beslut om vilka incidenter som ska rapporteras till ledningen
- Åtgärdsplan för informationssäkerhet
- Kontinuitetsplan
- Utsedd person med övergripande och samordnande ansvar för myndighetens informationssäkerhet
- Internetpolicy
- Distansarbetspolicy
- E-postpolicy
- Åtkomstpolicy[8]
- Process för säkerhetskopiering av all verksamhetskritisk information
- Process för styrning av utveckling/förändringar i IT-miljö, IT-system och bemanning

[5] Exempelvis säkerhetschef, systemägare, användare, IT-styrgrupp m fl

[6] Om det exempelvis inte sker något distansarbete så behövs givetvis ingen distansarbetspolicy.

[7] En del komponenter tas upp i särskilda avsnitt, bl.a. riskanalys och de som avser utbildning och information och medtas därför inte i denna uppställning

[8] Policy som reglerar åtkomst av informationstillgångar

- Processer för återkommande uppföljning och förvaltning av LIS

Dessa bör vara dokumenterade, beslutade och införda i verksamheterna. De bör vara utformade utifrån myndighetens särskilda behov och därvid beakta relevant best practice[9] inom aktuellt område.

Komponenterna bör utgöra en lämpligt utformad helhet – som i sin tur bör utgöra en integrerad del i myndighetens totala ledningssystem.

Iakttagelser och bedömningar från granskningen

Riksrevisionen har kunnat konstatera att de områden som berörs under stycket Bedömningskriterier ovan, i allt väsentligt har beaktats av Försvarsmakten. Informationen är inte alltid samlad i specifika policydokument, utan kan beröras i flera olika styrande dokument, vilka sammantaget representerar Försvarsmaktens ställningstagande inom respektive område. Det kan emellertid göra det svårt för medarbetarna att överblicka och därmed beakta alla inriktningsbeslut. I nedanstående avsnitt kommenteras inte vart och ett av de områden som angivits ovan, utan enbart vissa punkter som bedöms vara av särskilt intresse.

Försvarsmaktens rutiner och kontroller vid *tilldelning* av behörigheter i IT-miljön synes utifrån den genomförda granskningen vara tillfredsställande. Riksrevisionen har dock noterat att generella rutiner för *avveckling* av användare som ej längre skall ha behörighet, eller som skall byta behörighet i applikationer och nätverk, kan förbättras. Riksrevisionens tolkning av det nuvarande regelverket är att det i lokala riktlinjer skall fastställas hur borttag av behörigheter skall hanteras. Erfarenhetsmässigt bedömer Riksrevisionen detta som ett riskområde som bör åtgärdas, exempelvis genom att inrätta/föreskriva en generell rutin där personalansvarig funktion på förband eller motsvarande, åläggs att meddela den funktion som ansvarar för behörighetsadministration när en anställd lämnar organisationen. Riksrevisionen bedömer detta som särskilt viktigt med tanke på att Försvarsmakten fortfarande är inne i en process där ett inte oväsentligt antal anställda lämnar organisationen, eller byter organisatorisk tillhörighet inom myndigheten.

Riksrevisionen har vidare noterat att det idag på några områden saknas tillgängliga programvaror för skydd av informationstillgångar, och för vilka ett behov upplevs i verksamheten. Detta gäller främst vissa verktyg för logganalys, samt kryptering av hårddiskar. Avseende logganalys finns verktyg som godkänts för användning mot system, men som inte kan eller får tillämpas generellt inom myndigheten. Upphandling av en krypteringsprogramvara har avslutats och Försvarsmakten anger att planerat införande sker under 2006.

Riksrevisionen bedömer att rutinerna för kontinuitetsplanering vid Försvarsmakten kan förbättras. Den information som erhållits vid granskningen är att kontinuitetsplaneringen inte alltid baseras på dokumenterade analyser av hur länge verksamheten kan fortgå utan tillgång

[9] Myndigheten bör alltså informera sig om och dra nytta av de kunskaper som finns i standards såsom SIS 17799, NISTs 800-serie av rapporter mfl.

till applikationer och nätverksresurser, utan i flera fall baseras på övergripande uppskattningar. Riksrevisionen vill poängtera vikten av att verksamhetsansvariga ges möjlighet att aktivt delta i bedömningen av de krav som skall gälla för kontinuitetsplaneringen. Enligt uppgifter från Försvarsmakten skall kraven på informationstillgänglighet alltid finnas dokumenterade i ackrediteringsunderlaget för respektive tjänst innan tjänsten införs. Denna information bör då även kunna utgöra ett viktigt underlag för upprättande av kontinuitetsplan för verksamheten. Riksrevisionen har även under granskningen gjort bedömningen att förebyggande tester av kontinuitetsplanerna endast förekommer i mindre omfattning, vilket innebär en ökad risk att önskad servicenivå gentemot verksamheten inte kan uppnås i händelse av driftsstörningar mm. Som exempel kan nämnas att Försvarsmaktens vid upprättandet av delårsrapport 2005 inte kunde erhålla komplett information från vissa redovisningsenheter. Detta pga datorhaveri som uppstod i samband med bokslutsarbetet. Arbetet komplicerades ytterligare pga. att backup-rutinerna inte fungerat på avsett sätt, vilket innebar att informationen till bokslutstillfället till slut fick återskapas genom manuella rutiner.

Riksrevisionen bedömer att modellen för SLA (Service Level Agreements) kan utvecklas. Vid granskningen har framförts att den mall som för närvarande används för framtagande av SLA inte alltid, på ett tydligt och heltäckande sätt kan täcka in de behov, som finns från organisationsenheternas sida gentemot driftsansvariga enheter. Det har också påtalats att det i vissa fall kan råda oklarhet om ansvarsförhållandena i de fall där tillgänglighetsproblem uppstår och mer än en driftägare kan vara involverad.

Riksrevisionen kan generellt också konstatera att vissa informationssäkerhetsaspekter, såsom informationsklassificering och val av kommunikations- och lagringsmetoder, försvåras när man i samband med internationella övningar/insatser samutnyttjar informationsresurser med andra länder. Då denna typ av verksamhet sannolikt kommer att öka i framtiden är det viktigt att finna såväl policy som lösningar som på ett kostnadseffektivt sätt uppfyller de säkerhetskrav som ska ställas i dessa situationer. Riksrevisionen bedömer det också som viktigt att det i förväg definierats vilka rutiner som skall gälla, och vilken dokumentation som ska krävas, i de fall undantag måste tillämpas från de av Försvarsmakten beslutade regelverken.

Genomförda intervjuer visar slutligen att en stor mängd versioner av programvaror och operativsystem idag finns inom myndigheten. Detta innebär enligt Riksrevisionens bedömning en risk dels att uppdateringar idag inte kan administreras på ett kostnadseffektivt och säkerhetsmässigt tillfredsställande sätt, dels att myndigheten kan få svårt att överblicka vilka datorer som omfattas av ett givet säkerhetsproblem. Försvarsmakten har initierat flera projekt som syftar till konsolidering av IT-miljön, vilket framgent torde minska denna risk.

Sammantaget bedömer Riksrevisionen att de kontrollfunktioner som Försvarsmakten inrättat avseende sin informationssäkerhet ger förutsättningar för en god måluppfyllelse. Som konstaterats ovan finns dock vissa områden rörande bl.a. kontinuitetsplanering samt vissa aspekter av

behörighetshanteringen som kan utvecklas för att ytterligare höja nivån på Försvarsmaktens informationssäkerhetsarbete. De två områden som här exemplifieras är särskilt viktiga med tanke på den förändringsprocess som Försvarsmakten nu befinner sig i, med dels ett ökat beroende av informationstillgänglighet genom bl.a. NBF (Nätverksbaserat Försvar), dels omstruktureringen som gör att ett stort antal personer lämnar organisationen.

2.5 Information och utbildning

Bedömningskriterier

Information avser ledningens åtgärder för att förse personalen med relevant information och kunskaper angående myndighetens informationstillgångar, säkerhetsåtgärder, incidenter och ledningssystem för informationssäkerhet.

Det bör finnas en process för systematisk och återkommande information och utbildning beträffande informationssäkerhet till relevanta grupper[10]. Den bör innefatta de anställdas ansvar för informationssäkerheten samt de väsentliga hot och risker som ska beaktas i deras arbete.

Vidare bör det finnas en process för återkommande uppföljning av att IT-användarna är tillräckligt medvetna om och kompetenta att hantera hot och risker.

Iakttagelser och bedömningar från granskningen

Försvarsmakten ställer idag som krav att en användare skall ha genomgått informationssäkerhetsutbildning, för att få tillgång till Försvarsmaktens nätverk och applikationer. Detta område regleras i ett omfattande internt referensmaterial, och Riksrevisionen har inte heller sett några indikationer på brister inom området.

Av bl.a. H SÄK IT (kap 10.4) framgår att denna utbildning bör genomföras regelbundet. Riksrevisionen uppfattar dock en risk att *uppföljande samt kompletterande information och utbildning* inte alltid ges det utrymme som skulle vara önskvärt för att säkerställa att personalen har aktuell och uppdaterad kunskap. I detta sammanhang anser Riksrevisionen det vara viktigt att ett tydligt åtagande finns från olika ledningsnivåer inom organisationen, exempelvis genom de fastställda målsättningar för informationssäkerhetsarbete som enligt FMS VHL 2003 skall finnas på enhetsnivå. Riksrevisionen bedömer att denna typ av tydliga målformuleringar också ger en större legitimitet till att resurser för utbildning, information och uppföljning kontinuerligt kan avsättas i organisationen.

[10] Nyanställda, myndighetsledning, övriga chefer, övriga medarbetare.

2.6 Uppföljning och förvaltning

Bedömningskriterier

Uppföljningen bör vara en naturlig del av ledningens kontroll av att delegerad befogenhet hanteras på avsett sätt. Uppföljningen bör ske systematiskt och regelbundet genom av ledningen inrättade funktioner. Vid vissa tillfällen kan därutöver särskilda insatser vara påkallade i form av konsultuppdrag och andra utvärderings/kontrollinitiativ. Sådana insatser kan emellertid inte ersätta den systematiska och regelbundna uppföljningen.

Uppföljningen bör avse de kontrollobjekt som är av större betydelse för informationssäkerheten i myndighetens verksamhet såsom att

- riskanalysprocessen fungerar som avsett.
- åtgärdsplanering och genomförande fungerar som avsett.
- incidentrapporteringen fungerar som avsett.
- kontinuitetsplaneringen fungerar som avsett.
- e-posthanteringen fungerar som avsett.
- den interna kontrollen av förändringar i IT-miljön och personella resurser fungerar som avsett.
- den interna kontrollen av åtkomst av informationsresurser fungerar som avsett.
- distansarbetspolicyn fungerar som avsett.
- internetpolicyn fungerar som avsett.
- information och utbildning beträffande informationssäkerhet fungerar som avsett.
- den faktiskt uppnådda informationssäkerheten systematiskt prövas och uppfyller säkerhetskraven.

Resultaten från övervakningen utgör underlag för förvaltning och utveckling av myndighetens LIS. Ledningen bör ha infört en dokumenterad process för förvaltning och utveckling av sitt LIS.

Iakttagelser och bedömningar från granskningen

I de centrala styrdokumenten H SÄK IT samt H SÄK SKYDD anges ett antal olika typer av kontroller som kan, respektive skall genomföras vid Försvarsmakten (planlagda, periodiska och överraskande kontroller samt daglig tillsyn). Kontroller genomförs antingen på initiativ av organisationsenhetens chef, eller på initiativ av överordnad enhet. Lokala revisioner av verksamhetsledningssystemet skall dessutom, enligt FMS VHL 2003 genomföras regelbundet, och utgöra grund för processen ”Ledningens granskning”. De brister som iakttas vid de olika granskningarna skall dokumenteras.
Som konstaterats tidigare i rapporten anser Riksrevisionen att uppföljningen och förvaltningen av enstaka delmoment, som omnämns ovan under Bedömningskriterier, skulle kunna utvecklas. Detta avser exv. uppföljning av

kontinuitetsplaneringen, samt central uppföljning av återkommande riskanalyser i organisationen. Vidare visar granskningen att arbetet med att analysera och utvärdera resultatet av de olika kontroller och uppföljningar som genomförts av informationssäkerhetsarbetet kan förstärkas. En sådan process har nyligen tillskapats vid MUST, men har ännu inte tillämpats praktiskt i någon större omfattning.

Sammantaget bedömer Riksrevisionen dock att de granskning- och kontrollåtgärder som presenterats av Försvarsmakten ger en goda förutsättningar för ledningen att kunna bedöma och utvärdera informationssäkerhetsarbetet vid myndigheten. För att denna bedömning skall kunna utföras på ett effektivt sätt anser Riksrevisionen det dock vara väsentligt att processen för central analys och utvärdering av kontrollverksamheten införs i enlighet med den information som erhållits i samband med granskningen.

3. Slutsatser och rekommendationer

Som konstaterats ovan har Försvarsmakten ett omfattande centralt regelverk för informationssäkerhetsarbetet. Tillämpningen och införandet av ISO 17799 bör enligt Riksrevisionens bedömning underlättas av det ”Uttalande om tillämplighet” som framtagits, och som på ett tydligt sätt visar vilka detaljregelverk som är tillämpliga för respektive delområde i standarden. Genom införandet av informationssäkerhetsdimensionen i FMS VHL 2003 ges också en tydlig markering om ledningsperspektivet på informationssäkerhetsfrågorna, vilket erfarenhetsmässigt är en väsentlig faktor för ett bra resultat.

Ansvarsfördelningen inom Försvarsmakten innebär att det i väsentliga delar är produktägare och systemägare som ansvarar för att uppsatta mål för informationssäkerhetsarbetet faktiskt uppnås. Riksrevisionens bedömning är att detta decentraliserade ansvar ställer särskilda krav på aggregerad analys och sammanställning av det arbete som utförs lokalt, för att säkerställa att de krav som ställs på myndighetsledningen i bl.a. §6-7 Verksförordningen (1995:1322) uppfylls. Riksrevisionens *rekommendation* är att Försvarsmakten bör utveckla arbetet med central analys och sammanställning av de riskanalyser som genomförs lokalt. Riksrevisionen *rekommenderar* vidare att riskanalyserna tydligt fokuserar den process som skall stödjas av en viss produkt/ informationsmängd. Det finns en potentiell fara att risker som berör tvärgående processer kan förbises om fokus vid riskbedömningar är alltför inriktad på produkter och system i stället för på den process som informationen skall understödja. Detta exemplifieras dels av brister som under 2005 har uppdagats vad gäller kvaliteten i överföring av information från försystem till den finansiella redovisningen avseende värdet av Försvarsmaktens lagertillgångar, dels av att Riksrevisionen lämnade invändning i revisionsberättelsen 2004 avseende brister i hanteringen av Försvarsmaktens beredskapstillgångar, vilka bl.a. orsakas av bristande systemstöd.

Riksrevisionen har vid granskningen noterat vissa aktiviteter där vi *rekommenderar* att rutiner och processer bör förstärkas, för att ytterligare

förbättra skyddet vad gäller informationshanteringen vid Försvarsmakten. Detta gäller dels hanteringen av behörigheter för personal som lämnar myndigheten, vilket bedöms vara särskilt aktuellt pga. den pågående omstruktureringen av försvarets verksamhet. Det gäller även rutinerna för upprättande och test av kontinuitetsplanering, som Riksrevisionen anser bör utvecklas för att säkerställa att informationsresurser kan tillhandahållas i den omfattning som är nödvändigt för effektivt och säkert utförande av verksamheten. Slutligen har Riksrevisionen också noterat att det idag föreligger viss oklarhet rörande de åtaganden som interna leverantörer av tjänster har gentemot verksamheten, avseende såväl SLA (Service Level Agreements) som ansvarsfördelning mellan olika ägarroller.

Riksrevisionen *rekommenderar* vidare att Försvarsmakten bör utveckla arbetet med en kontinuerlig samlad analys, uppföljning och utvärdering av de kontroller och revisioner som utförs på olika nivåer i organisationen. En samlad analys och utvärdering ger enligt Riksrevisionens bedömning förbättrade möjligheter att såväl upptäcka behov av förändringar och kompletteringar i interna regelverk och kontrollfunktioner, som att iaktta områden som särskilt bör beaktas i kommande riskanalyser inom myndigheten.

På flera områden pågår förändringar som Riksrevisionen *rekommenderar* Försvarsmakten att särskilt beakta i förvaltningen av informationssäkerhetsarbetet. Detta gäller bl.a. den pågående konsolideringen av IT-miljön och de eventuella ändrade roller och ansvarsförhållanden som då kan uppstå. Det är särskilt viktigt att då beakta de *olika* verksamhetsbehov som skall lösas inom en process respektive applikation, vilket även noterats tidigare i denna rapport. Detsamma gäller även andra pågående förändringar av försvarets verksamhet, bl.a. vad gäller delvis förändrad verksamhetsinriktning, som också kan ställa nya krav på fördelning av roller och ansvar, inte minst i anslutning till ökade internationella åtaganden. Även strukturella och personella förändringar inom myndigheten är särskilt viktiga att beakta såväl vad gäller den förändrade riskbild som kan uppstå under förändringsperioden, som vid tillämpningen och omfattningen av olika kontroll- och uppföljningsaktiviteter. Detta för att säkerställa att informationssäkerhetsarbetet planeras, genomförs och följs upp på ett säkert och kostnadseffektivt sätt.

Revisionsdirektör Bengt Bengtsson har beslutat i detta ärende. Revisionsledare Frank Lantz har varit föredragande.

Bengt Bengtsson Frank Lantz

Bilaga:
Försvarsmakten IT-revision 2006-06-08 (rapport från Transcendent Group)

Kopia för kännedom:
Försvarsdepartementet