Verktygsstöd för hot-, risk- och sårbarhetsanalyser

Realiseringsförslag

JONAS HALLBERG, JOHAN BENGTSSON, TEODOR SOMMESTAD

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se

FOI-R--3552--SE
ISSN 1650-1942

December 2012

Jonas Hallberg, Johan Bengtsson,
Teodor Sommestad

Verktygsstöd för hot-, risk- och sårbarhetsanalyser

Realiseringsförslag

Bild/Cover: Johan Bengtsson

Titel	Verktygsstöd för hot-, risk- och sårbarhetsanalyser – Realiseringsförslag
Title	Tools supporting threat and risk analyses – Implementation proposals
Rapportnr/Report no	FOI-R--3552--SE
Månad/Month	December
Utgivningsår/Year	2012
Antal sidor/Pages	43 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten
FoT område	Ledning och MSI
Projektnr/Project no	E36017
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Genomförandet av hot-, risk- och sårbarhetsanalyser för planerade IT-system är centralt för Försvarsmaktens samlade informationssäkerhet. Det finns många behov av stöd vid genomförandet av dessa analyser. En uppsättning sådana behov har identifierats under tidigare genomförd behovsanalys.

I denna rapport presenteras över 20 förslag vars realisering skulle tillfredsställa många av de identifierade behoven av stöd. Förutom de identifierade behoven har demonstratorn Sublime utgjort en utgångspunkt vid framtagandet av realiseringsförslagen. Sublime är en demonstrator som utformats för att stödja analysarbete som genomförs enligt Försvarsmaktens gemensamma riskhanteringsmodell. Det arbete som krävs för att realisera förslagen är av varierande omfattning. Tidsåtgången påverkas också av vilka ansatser som väljs vid realiseringen. En komplettering av demonstratorn Sublime bedöms dock inte kräva större insats än några personmånader för något av realiseringsförslagen.

Utöver realiseringsförslagen har över 20 forskningsfrågor identifierats inom sex olika områden, såsom *automatiserad riskbedömning* och *balans mellan nytta och risk*. Framtida studier av forskningsfrågorna kan ge kunskap av betydelse för utvecklingen av de analyser som ligger till grund för den säkerhetsmålsättning som tas fram för Försvarsmaktens IT-system.

I det fortsatta arbetet, under 2013, kommer realiseringsförslagen att prioriteras i den ordning som ger största möjliga effekt med hänsyn till tillgängliga resurser. Därefter påbörjas realiseringen av den demonstrator, baserad på Sublime, som ska levereras till Försvarsmakten i slutet av 2013. Någon eller några av de identifierade forskningsfrågorna kan komma att adresseras under 2013, men de utgör framförallt en grund för kommande forskningsprojekt och det fortsatta arbetet inom området.

Nyckelord: Hotanalys, riskanalys, sårbarhetsanalys, IT-säkerhet, säkerhetskrav, säkerhetsmålsättning

Summary

The threat and risk analyses performed for planned IT systems are crucial for the information security of the Swedish Armed Forces. There are many needs for supporting methods and tools during these analyses. A set of such needs has been specified through previously performed needs analyses.

This report presents more than 20 suggestions whose implementation would satisfy many of the identified needs. In addition to the identified needs, the demonstrator Sublime has been a starting point for the suggestions. The purpose of Sublime is to illustrate a possible design of tools supporting the analyses based on the Common Risk Management Model of the Swedish Armed Forces. The effort required to implement the suggestions differs. The level of effort required also depends on the specific approach selected for the implementation of a suggestion.

In addition to the implementation suggestions, more than 20 research questions have been identified. Future studies of these research questions have the potential to fundamentally affect the bases and the execution of the threat and risk analyses.

Future work, during 2013, will include the prioritization of the suggestions and the implementation of a set of high-priority suggestions. Some of the research suggestions may also be addressed. However, the specified research questions are, foremost, a basis for future research projects.

Keywords: Threat analysis, risk analysis, IT security, security requirement

Innehåll

1 Inledning

Auktorisation och ackreditering av IT-system är en central del av Försvarsmaktens IT-säkerhetsarbete. Som underlag för ett av delbesluten under auktorisationen utformas en säkerhetsmålsättning för varje planerat IT-system.

En säkerhetsmålsättning är en sammanställning av bland annat hotbilden, gjorda riskbedömningar och de IT-säkerhetskrav som kommer att ställas på IT-systemet. En viktig del i arbetet med säkerhetsmålsättningar är därför att genomföra hot-, risk- och sårbarhetsanalyser för att identifiera och bedöma hot, risker och sårbarheter associerade med IT-system.

Under 2012 har en behovsanalys genomförts för att identifiera behov av stöd under de hot-, risk- och sårbarhetsanalyser som genomförs som en del i arbetet med att ta fram säkerhetsmålsättningar. Behovsanalysen[1] visar att det finns många sådana behov.

1.1 Syfte

Syftet med denna rapport är att beskriva realiseringsförslag som kan leda till mer systematiskt och effektivt genomförande av de hot-, risk- och sårbarhetsanalyser som ligger till grund för säkerhetsmålsättningar för Försvarsmaktens IT-system. Utöver realiseringsförslagen har ett antal forskningsfrågor identifierats. Såväl realiseringsförslagen som forskningsfrågorna relaterar även till andra aktiviteter som genomförs före eller efter hot-, risk- och sårbarhetsanalyser. Dessa tillkommande aktiviteter är nödvändiga för att det ska finnas adekvat underlag för hot-, risk-, och sårbarhetsanalyser respektive att de erhållna resultaten tas om hand. Verksamhetsanalys och formulering av säkerhetskrav utgör exempel på sådana aktiviteter. I denna rapport används benämningen *närliggande arbetsuppgifter* som beteckning för dessa aktiviteter.

Ett grundläggande antagande är att tillgången till verktygsstöd har en stor betydelse för strävan mot att tillfredsställa de behov användarna har avseende hot-, risk- och sårbarhetsanalyser. Problem gällande avsaknaden av instruktioner och struktur inom området är centrala delar som ett verktygsstöd behöver omfatta för att stödja användarna i deras arbete med hot-, risk- och sårbarhetsanalyser.

[1] J Bengtsson, K Lundholm, J Hallberg. (2012). *Behov av stöd vid genomförande av hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarsmakten*. FOI-R--3452--SE.

1.2 Bidrag

Det arbete som beskrivs i denna rapport utförs inom ramen för FoT-projektet *Effektivare hot-, risk- och sårbarhetsanalyser*. Målet med projektet är att ta fram en demonstrator för att påvisa hur arbetet med hot-, risk- och sårbarhetsanalyser samt närliggande arbetsuppgifter skulle kunna effektiviseras inom Försvarsmakten. Detta både för analysgruppen som genomför analyserna och för de som granskar och fattar beslut baserat på resultaten.

I denna rapport presenteras:

- över 20 realiseringsförslag avseende verktygs- och metodstöd för genomförande av hot-, risk- och sårbarhetsanalyser samt närliggande arbetsuppgifter
- över 20 forskningsfrågor relaterade till hot-, risk- och sårbarhetsanalyser samt närliggande arbetsuppgifter.

Dessa realiseringsförslag och forskningsfrågor utgör en grund för vidare arbete som syftar till att tillfredsställa behov av stöd vid genomförande av hot-, risk, och sårbarhetsanalyser och närliggande arbetsuppgifter.

1.3 Läsanvisning

I kapitel 2 ges övergripande beskrivningar av Försvarsmaktens gemensamma riskhanteringsmodell och Sublime. Sublime är en demonstrator för genomförande av hot-, risk- och sårbarhetsanalyser i enlighet med Försvarsmaktens gemensamma riskhanteringsmodell.

I kapitel 3 beskrivs kortfattat tidigare identifierade behov relaterade till stöd vid genomförande av hot-, risk- och sårbarhetsanalyser för Försvarsmaktens IT-system samt det urval som genomförts avseende dessa behov.

I kapitel 4 beskrivs de framtagna realiseringsförslagen avseende verktygs- och metodstöd.

I kapitel 5 beskrivs forskningsfrågor relaterade till hot-, risk- och sårbarhetsanalyser samt närliggande arbetsuppgifter.

Rapporten avslutas med en beskrivning av det fortsatta arbetet i kapitel 6.

2 Hot-, risk- och sårbarhetsanalys

I dagsläget utgår arbetet med auktorisation och ackreditering av Försvarsmaktens IT-system från IT-livscykelmodellen i DIT 04[2]. I steg två i IT-livscykelmodellen ska säkerhetsmålsättning för aktuellt system tas fram. Genomförandet av hot-, risk- och sårbarhetsanalyser är en av de viktigaste delarna i arbetet att ta fram en säkerhetsmålsättning och utgår i huvudsak från H SÄK IT[3]. Ett problem är att det saknas en fastställd metod för *hur* analyserna ska genomföras[4]. Detta resulterar i att analyserna genomförs på olika sätt beroende på vem som leder arbetet.

Vid arbetet med att ta fram realiseringsförslag är det nödvändigt att utgå från en strukturerad metod för genomförande av hot-, risk- och sårbarhetsanalyser. Utgångspunkten för arbetet för arbetet som presenteras i denna rapport är Försvarsmaktens gemensamma riskhanteringsmodell. Detta beslut grundas på att Försvarsmaktens gemensamma riskhanteringsmodell är fastställd samt kan och bör användas för att hantera risker i Försvarsmaktens verksamhet[5].

Försvarsmaktens gemensamma riskhanteringsmodell fastslogs den första januari 2009 och består av följande fem steg:

1. Fastställ grundvärden
2. Konkretisera och bedöm hoten
3. Identifiera skydd och bedöm sårbarheter
4. Bedöm risken
5. Riskhanteringsbeslut med plan för uppföljning

Vid framtagandet av riskhanteringsmodellen har fokus legat på att ta fram en beskrivning där det inte bara tydligt framgår *vem* som ska göra *vad* i varje steg, utan även *hur*. I dagsläget används Försvarsmaktens gemensamma riskhanteringsmodell mestadels för riskanalyser relaterade till militära insatser, men inga hinder finns för att använda den inom andra områden som exempelvis för IT-system.

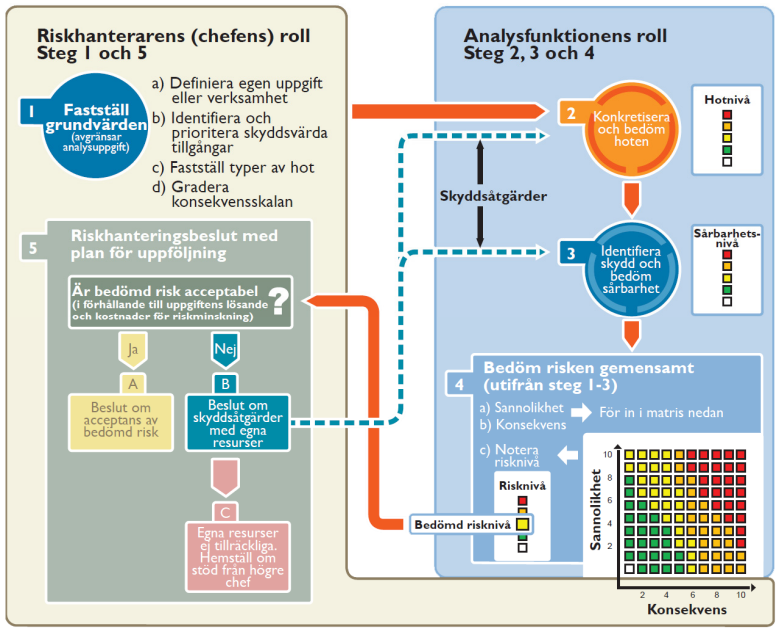
Sublime är en demonstrator som tagits fram av FOI i samarbete med FMKE. Syftet med Sublime är att påvisa hur ett verktygsstöd kan utformas för att stödja det analysarbete som genomförs med hjälp av Försvarsmaktens gemensamma riskhanteringsmodell (Figur 1).

---

[2] Försvarsmakten. (2004). *Direktiv för Försvarsmaktens Informationsteknikverksamhet (DIT 04)*.
[3] Försvarsmakten. (2006). *Handbok för Försvarsmaktens säkerhetstjänst, informationsteknik (H SÄK IT)*. M7745-734062.
[4] J Bengtsson, K Lundholm, J Hallberg. (2012). *Behov av stöd vid genomförande av hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarsmakten*. FOI-R--3452--SE.
[5] Försvarsmakten. (2009). Försvarsmaktens gemensamma riskhanteringsmodell. M7739-350012.

Sublime är helt baserad på Försvarsmaktens handbok[6] som beskriver riskhanteringsmodellen. Inga anpassningar har gjorts av Sublime för att specifikt stödja analyser av IT-system.

Den nedanstående beskrivningen av Försvarsmaktens gemensamma riskhanteringsmodell och Sublime grundar sig på den beskrivning som tidigare tagits fram i form av ett rapportunderlag till FMKE.



Figur 1: Översikt av Försvarsmaktens gemensamma riskhanteringsmodell[6].

2.1 Steg 1 – Fastställ grundvärden

Det initiala steget i Försvarsmaktens gemensamma riskhanteringsmodell syftar till att besluta om inriktning samt avgränsningar för det fortsatta arbetet. Inriktning och avgränsningar fastställs genom att specificera följande fyra grundvärden.

1. Definiera verksamheten samt avgränsningar i tid, geografi och tema.
2. Identifiera och prioritera skyddsvärda tillgångar.
3. Fastställ vilka typer av hot som ska analyseras.

[6] Försvarsmakten. (2009). Försvarsmaktens gemensamma riskhanteringsmodell. M7739-350012.

4. Fastställ konsekvensskalor för de typer av hot som ska analyseras.

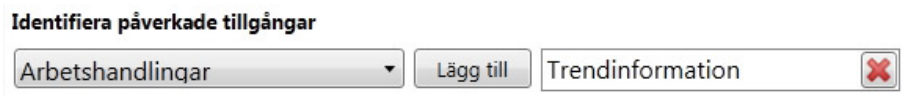
Detta steg ska genomföras av ansvarig chef. Oavsett om det är chefen eller staben som i praktiken genomför detta arbete så är det alltid chefen som fastställer de grundvärden som ska användas i de följande stegen.

Resultatet av steg 1 är följande grundvärden:

- verksamhetsbeskrivning
- lista över skyddsvärda tillgångar
- lista över typer av hot att beakta
- konsekvensskalor.

2.2 Steg 2 – Konkretisera och bedöm hot

De typer av hot som fastställts i steg 1 konkretiseras i detta steg till konkreta hot. De konkreta hoten ska vara på en sådan nivå att det går att förhålla sig till dem ur ett skydds- och sårbarhetsperspektiv. För varje hot anges vilka skyddsvärda tillgångar som kan påverkas. Hur detta ser ut i Sublime återges i Figur 2. En femgradig skala används för att bedöma hotnivån[7] för varje specifikt hot, där 1 betyder *inget synbart hot* och 5 betyder *mycket högt hot*. Varje värde på skalan har även en tillhörande färg för att tydligt kunna illustrera tilldelad hotnivå grafiskt. Hur detta ser ut i Sublime återges i Figur 3.



Figur 2: Exempel på hur de skyddsvärda tillgångar som kan påverkas kopplas till ett konkret hot.

Den tilldelade hotnivån återspeglar inte sannolikheten för att hotet ska inträffa, utan är en bedömning av hotet i den kontext i vilken den definierade verksamheten ska utföras. Sannolikheten att ett specifikt hot inträffar bedöms istället i steg 4, efter att hänsyn har tagits till faktorer såsom exponering, skyddsnivå och effekt av skyddsåtgärder.

Resultatet av steg 2 är en uppsättning konkreta hot.

[7] ”En hotnivå avseende ett antagonistiskt hot är en samlad bedömning av en eller flera aktörers intention, kapacitet och tillfälle i tid och rum att bruka ett visst offensivt eller defensivt modus operandi för att i direkt, indirekt eller överförd bemärkelse påverka en skyddsvärd tillgång och därigenom förorsaka en oönskad händelse.” (Försvarsmakten. (2009). *Försvarsmaktens gemensamma riskhanteringsmodell*. M7739-350012)

Figur 3: Val av hotnivå i Sublime, med nivå 4 vald.

2.3 Steg 3 – Identifiera skydd och bedöm sårbarheter

I detta steg specificeras det skydd som finns mot de hot som identifierats i steg 2. Skydd definieras som den samlade förmågan att skydda en skyddsvärd tillgång mot ett hot. Skyddet består av en eller flera skyddsåtgärder. Det finns ett flertal olika typer av skyddsåtgärder att tillgå. Syftet med dem är dock alltid att minska sannolikheten att ett eller flera hot inträffar och/eller konsekvensen av dem.

Sårbarhetsnivån bedöms för varje kombination av hot och tillgång med avseende på aktuell skyddsåtgärd. Varje sårbarhet skattas med ett värde i intervallet 1 till 5, där 1 betyder ingen synbar sårbarhet och 5 betyder mycket hög sårbarhet. På samma sätt som vid bedömningen av hotnivå så finns en tillhörande färg för att tydligt kunna illustrera tilldelad sårbarhetsnivå grafiskt. Hur detta ser ut i Sublime återges i Figur 4.

Resultatet av steg 3 är en uppsättning skyddsåtgärder med bedömda sårbarhetsnivåer.

Hot	Tillgång	Sårbarhetsnivå
Stöld av trendinformation (Hot mot informationstillgångar)	Trendinformation	
Förvanskning av beslut (Hot mot informationstillgångar)	Riktighet på beslut	
Stöld av arbetshandlingar (Hot mot informationstillgångar)	Arbetshandlingar	
Tillgänglighetsangrepp (Hot mot informationstillgångar)	Tillgänglighet	

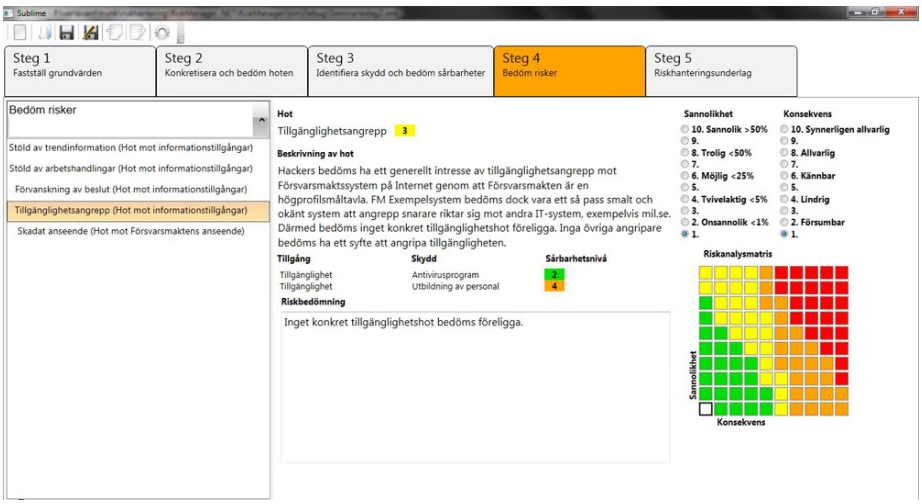
Figur 4: Specificering av sårbarhetsnivå för kombinationer av hot och tillgång som påverkas av aktuell skyddsåtgärd.

2.4 Steg 4 – Bedöm risker

Med det resulterande underlaget från steg 2 och 3 bedöms risken associerad med vart och ett av de konkreta hoten. Dessa bedömningar görs gemensamt av den analysgrupp som har arbetat med att ta fram underlaget i de två tidigare stegen. Riskbedömningen består av sannolikheten att det konkreta hotet ska inträffa samt konsekvensen om det inträffar. Hur detta ser ut i Sublime återges i Figur 5.

Sannolikheten skattas med ett värde i intervallet 1 till 10 baserat på den i handboken definierade sannolikhetsskalan. Konsekvensen om ett konkret hot skulle inträffa skattas enligt den konsekvensskala som fastslagits av chefen i metodens inledande steg. Dessa två värden förs sedan in i handbokens riskanalysmatris, ur vilken risknivån kan utläsas.

Resultatet av steg 4 är en uppsättning risker som motsvarar de konkreta hoten.



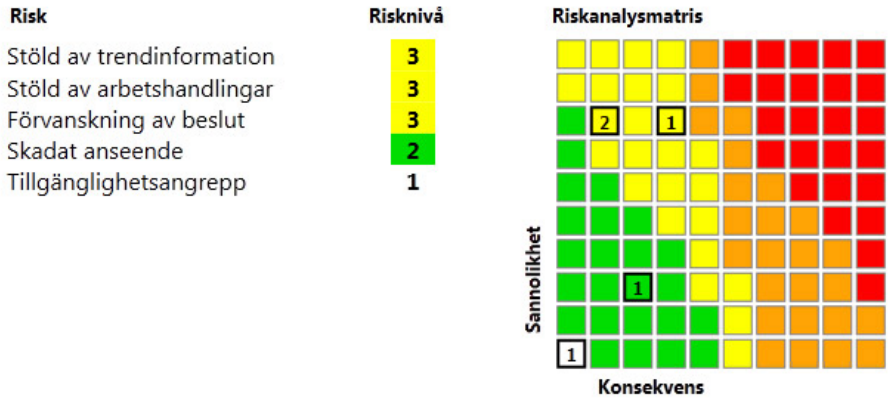
Figur 5: Bedömning av risker i Sublime.

2.5 Steg 5 – Riskhanteringsunderlag

I steg 5 i Försvarsmaktens gemensamma riskhanteringsmodell ska ansvarig chef fatta ett riskhanteringsbeslut utgående från resultaten från steg 1 till 4. I Sublime visualiseras istället resultaten från steg 1 till 4. I Sublime finns möjlighet att presentera resultaten på två olika sätt.

Det första sättet ger en övergripande bild av analysresultaten genom att presentera alla risker tillsammans med den bedömda risknivån. För att ytterligare förtydliga resultaten visas även riskanalysmatrisen där alla risker återges för att ge en överblick över hur allvarliga de bedömda riskerna är. Exempel på hur detta kan se ut återges i Figur 6.

Det andra sättet ger en mer detaljerad version av analysresultaten och stöttar analysgruppen genom att presentera analysresultaten i form av ett rapportunderlag i Word-format. Det är möjligt att välja vilka delar av analyserna som ska tas med i rapportunderlaget. I Figur 7 återges ett exempel på hur en del av rapportunderlaget kan se ut.



Figur 6: Resultat av genomförd analys i Sublime.

FÖRSVARSMAKTEN
HÖGKVARTERET

Titel/Rubrik | Sida

Enhet/Projekt/Arbetsgrupp | Datum 2012-11-26 | Beteckning

Handläggare | Godkänd av | Signatur | Version

3 Skydd

I detta kapitel bedöms nuvarande skydd och värderas därefter mot de konkreta hot som beskrivs i kapitel 2. Skydden syftar till att minska sannolikheten för och/eller konsekvensen av ett visst hot. Värderingen av skyddsförmågan mot respektive konkret hot resulterar i en sårbarhetsbedömning som skattas med ett värde 1-5 där 1 står för "ingen synbar sårbarhet" och 5 står för "mycket hög sårbarhet".

3.1 Antivirusprogram

Viruskontroll av samtliga filer som importeras. Rutin för att virusskyddet hålls uppdaterat. Ursprungskontroll och test med systemuppdatering. Backup med redundans.

Typ av skydd: **Aktivt**

Hot	Skyddad tillgång	Sårbarhetsnivå
Stöld av trendinformation	Trendinformation	2
Förvanskning av beslut	Riktighet på beslut	2
Stöld av arbetshandlingar	Arbetshandlingar	2
Tillgänglighetsangrepp	Tillgänglighet	2

3.2 Kryptering

Trafik krypterad med kommersiellt krypto, tillåt endast kommunikation med godkända protokoll.

Typ av skydd: **Passivt**

Hot	Skyddad tillgång	Sårbarhetsnivå

Figur 7: Exempel på rapportunderlag från Sublime.

3 Resultat från behovsanalys

Under 2011 genomfördes en behovsanalys för att klargöra vilka behov av stöd som finns vid genomförande av hot-, risk- och sårbarhetsanalyser inom Försvarsmakten[8]. Behovsanalysen baserades på sju intervjuer med personer från Försvarsmakten och FMV. Utöver dessa intervjuer analyserades även handböcker och relaterade föreskrifter från Försvarsmakten. Under 2012 kompletterades behovsanalysen med underlag från ytterligare intervjuer[9]. Behoven inordnades också i en ny struktur. Detta resulterade i en uppsättning med 32 behov fördelade på de fem kategorierna:

- Organisatoriska förutsättningar
- Tillvägagångssätt
- Kunskap
- Stöd vid bedömningar
- Analysresultat.

20 av de identifierade behoven har valts ut som utgångspunkt för arbetet med att ta fram realiseringsförslag. De realiseringsförslag som har utarbetats syftar till att tillgodose ett eller flera av dessa 20 behov, som återges nedan.

1. Behov av förståelse för varför analyserna genomförs.
2. Behov av att koordinera analyser för olika IT-system mellan vilka det finns beroenden.
3. Behov av egen personal inom Försvarsmakten som har tid och kompetens att genomföra analyserna.
4. Behov av att representanter från alla berörda delar av organisationen deltar i analysarbetet.
5. Behov av engagemang och intresse från ledningen.
6. Behov av ett arbetssätt som beaktar de hot som är specifika för aktuellt IT-system.
7. Behov av att analysarbetet genomförs enligt fastställda metoder.
8. Behov av ett arbetssätt som kan anpassas så att det står i proportion till IT-systemets omfattning.

[8] K Lundholm, J Bengtsson, J Hallberg. (2011). *Hot-, risk- och sårbarhetsanalys - Grunden för IT-säkerhet inom Försvarsmakten*. FOI-R--3349--SE.

[9] J Bengtsson, K Lundholm, J Hallberg. (2012). *Behov av stöd vid genomförande av hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarsmakten*. FOI-R--3452--SE.

9. Behov av instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram.
10. Behov av instruktioner och arbetssätt som stämmer överens med varandra.
11. Behov av arbetssätt som tillvaratar tillgänglig information om det planerade IT-systemet.
12. Behov av att de antaganden och bedömningar som görs under analysarbetet motiveras.
13. Behov av att icke avsiktliga hot beaktas vid genomförandet av hotanalysen.
14. Behov av stöd för att avgöra hur implementationen av föreslagna säkerhetskrav påverkar identifierade risker.
15. Behov av en fastslagen hotlista som kan användas som utgångspunkt vid genomförande av analyserna.
16. Behov av stöd för att bedöma sannolikhet för realisering av hot.
17. Behov av stöd för att bedöma konsekvens vid realisering av hot.
18. Behov av spårbarhet för de antaganden som görs under analyserna.
19. Behov av analysresultat som gör det möjligt att bedöma om det planerade IT-systemet kommer att kunna ackrediteras.
20. Behov av analysresultat som visar vilka risker som kommer att tas vid användning av det planerade IT-systemet.

4 Realiseringsförslag

De identifierade behoven av stöd (kapitel 3) samt demonstratorn Sublime (kapitel 2) har varit utgångspunkten vid framtagandet av de realiseringsförslag som presenteras i detta kapitel. Realiseringsförslagen har strukturerats efter den del av analysarbetet som förslaget berör. Detta resulterade i åtta områden som presenteras i avsnitt 4.1 till 4.8. Varje avsnitt inleds med en beskrivning av området följt av de behov som realiseringsförslagen bedöms tillfredsställa.

Vart och ett av realiseringsförslagen presenteras med avseende på problemet de adresserar, hur de kan realiseras och vilka beroenden som finns till andra realiseringsförslag. Alla realiseringsförslag som presenteras i detta kapitel är beskrivna på en övergripande nivå och av en omfattning att de, var för sig, bedöms möjliga att realisera inom ramen för detta forskningsprojekt.

4.1 Verksamhetsanalys

De verksamhetsanalyser som ligger till grund för hot-, risk, och sårbarhetsanalyser syftar till att lyfta fram de egenskaper hos verksamheten som är viktiga för analyserna. Det är viktigt att ha en tydlig förståelse för verksamheten för att hot-, risk- och sårbarhetsanalysen ska kunna ge relevanta resultat.

Realiseringsförslagen avseende verksamhetsanalys presenteras i avsnitt 4.1.1 till 4.1.3. Tabell 1 innehåller en överblick av de behov som realiseringsförslagen bedöms kunna tillfredsställa.

Tabell 1: Koppling mellan behov och realiseringsförslag relaterade till verksamhetsanalys.

Behov	Strukturerade formulär	Nyttjande av befintliga verksamhetsbeskrivningar	Uppdatering och godkännande
Förståelse för varför analyserna genomförs	X	X	X
Att koordinera analyser för olika IT-system mellan vilka det finns beroenden		X	X
Engagemang och intresse från ledningen			X

Behov	Strukturerade formulär	Nyttjande av befintliga verksamhetsbeskrivningar	Uppdatering och godkännande
Ett arbetssätt som beaktar de hot som är specifika för aktuellt IT-system	X	X	X
Att analysarbetet genomförs enligt fastställda metoder	X	X	X
Spårbarhet för de antaganden som görs under analyserna			X
Analysresultat som gör det möjligt att bedöma om det planerade IT-systemet kommer att kunna ackrediteras	X	X	X

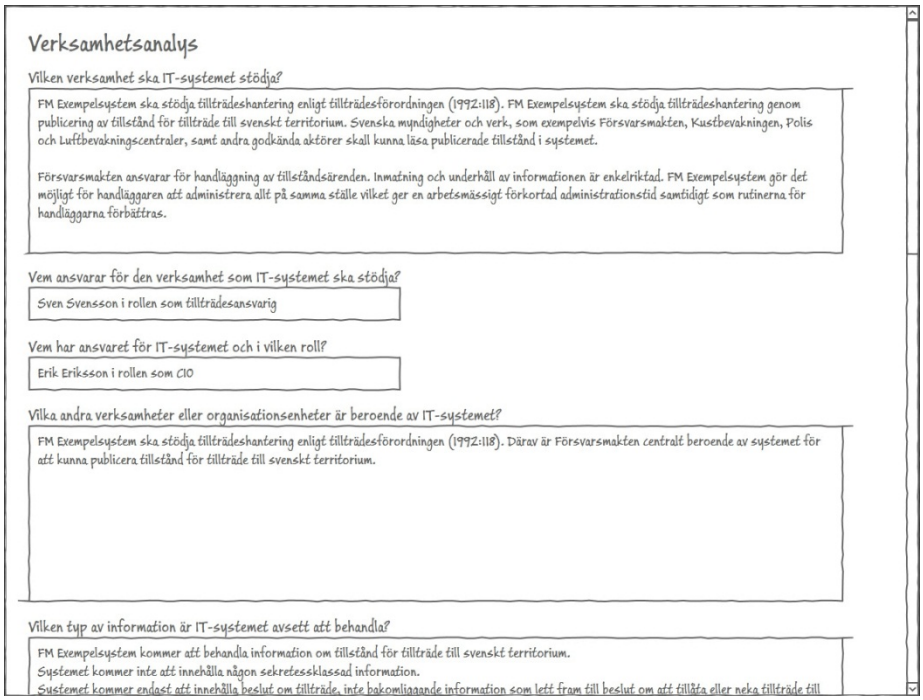
4.1.1 Strukturerade formulär

För att verksamhetsanalyser i förväg ska kunna sammanställa den information som det finns behov av vid hot-, risk- och sårbarhetsanalysen krävs kunskap om dessa behov. I dagsläget genomförs verksamhetsanalyser utifrån den mall som presenteras i MAACK[10]. I Sublime beskrivs verksamheten med hjälp av ett fritextfält.

För att förbättra förutsättningarna för verksamhetsanalyser kan fritextfältet i Sublime bytas ut mot ett formulär där användaren får svara på specifika frågor. På så sätt vägleds användaren att ange den information om verksamheten som förväntas. Det är då även möjligt att säkerställa att verksamhetsbeskrivningen faktiskt har förväntat innehåll. Figur 8 visar hur ett sådant formulär kan utformas.

I remissversionen av H Säk Infosäk[11] ges förslag på frågor som en verksamhetsanalys bör besvara. Dessa frågor utgör ett bra underlag för framtagandet av ett formulär. Det finns även delar i H Säk Grunder som bör beaktas.

[10] Försvarsmakten. (2007). *MAACK – Metod- & utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten*.
[11] Avsnitt 18.2 i remissutgåvan av H Säk Infosäk (Bilaga 1 till 2012-07-05 HKV 10 700:61060)



Figur 8: Skiss på hur formuläret för verksamhetsanalysen skulle kunna utökas.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.1.2 Nyttjande av befintliga verksamhetsbeskrivningar

När en säkerhetsmålsättning ska tas fram kan det sedan tidigare finnas beskrivningar av aktuell verksamhet. Dessa beskrivningar bör då återanvändas och således utgöra utgångspunkten för aktuell verksamhetsbeskrivning. Inriktningen för verksamhetsanalyserna är sannolikt olika och således är det väsentligt att kunna importera såväl som extrahera resultat från analyser i Sublime.

Sublime kan stödja nyttjande av befintliga verksamhetsbeskrivningar genom att:

- möjliggöra import av tidigare framtagna beskrivningar
- extrahera information från importerade beskrivningar
- komplettera och modifiera importerade beskrivningar.

Beroenden

Detta realiseringsförslag har beroenden till de realiseringsförslag som anges i tabellen nedan.

Tabell 2: Beroenden för realiseringsförslag *Nyttjande av befintliga verksamhetsbeskrivningar*.

ID	Namn
4.1.1	Strukturerade formulär

4.1.3 Uppdatering och godkännande

Enligt såväl Försvarsmaktens gemensamma riskhanteringsmodell som beskrivningar av processen för auktorisation och ackreditering av Försvarsmaktens IT-system, ska verksamhetsanalysen genomföras innan hot-, risk- och sårbarhetsanalysen. Detta medför att beskrivningar av verksamheter fastställs innan hot-, risk- och sårbarhetsanalyser genomförs.

Då verksamhetsbeskrivningar uppdateras under genomförandet av hot-, risk- och sårbarhetsanalysen ska dessa förändringar bekräftas av de som har fastställt de tidigare beskrivningarna. Om inte resultaten från verksamhetsanalysen uppdateras, kommer nyttjande av kompletterande information om verksamheten att leda till brist på konsistens mellan verksamhetsbeskrivningen och resultaten från de hot-, risk- och sårbarhetsanalyserna.

Sublime kan stödja uppdatering och godkännande av verksamhetsbeskrivningar genom att:

- verksamhetsbeskrivningar som tas fram måste godkännas av ansvarig chef, vilket överensstämmer med Förvarsmaktens gemensamma riskhanteringsmodell
- uppdateringar av verksamhetsbeskrivningar som görs under hot-, risk- och sårbarhetsanalyser markeras tydligt och ska godkännas separat
- slutgiltiga verksamhetsbeskrivningarna kan exporteras från verktyget för återkoppling till eventuella andra analyser som bedrivs parallellt med arbetet med säkerhetsmålsättningen.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.2 Författningsanalys

Författningsanalysen syftar till att analysera vilka föreskrifter som måste beaktas vid framtagandet av IT-system inom Försvarsmakten. Resultat från analysen används som underlag vid framtagandet av säkerhetsmålsättning för IT-system.

I dagsläget är det inte ovanligt att resultatet från en författningsanalys är en lång avskrift av alla tillämpliga paragrafer[12]. Detta är något som sällan tillför något mervärde till det fortsatta arbetet med säkerhetsmålsättningen.

Realiseringsförslagen avseende författningsanalys presenteras i avsnitt 4.2.1 till 4.2.2. Tabell 3 visar de behov som realiseringsförslagen bedöms kunna tillfredsställa.

Tabell 3: Koppling mellan behov och realiseringsförslag relaterade till författningsanalys.

Behov	Koppling mellan föreskrifter och analyser	Förslag på relevanta författningar
Förståelse för varför analyserna genomförs	X	X
Att analysarbetet genomförs enligt fastställda metoder	X	X
Instruktioner och arbetssätt som stämmer överens med varandra	X	X
Spårbarhet för de antaganden som görs under analyserna	X	X
Analysresultat som gör det möjligt att bedöma om det planerade IT-systemet kommer att kunna ackrediteras	X	X

4.2.1 Koppling mellan föreskrifter och analyser

De långa avskrifter av tillämpliga paragrafer som många författningsanalyser resulterar i tillför oftast inte något till det fortsatta analysarbetet. Detta medför att

[12] Avsnitt 18.3 i remissutgåvan av H Säk Infosäk (Bilaga 1 till 2012-07-05 HKV 10 700:61060)

det blir svårt att säkerställa att planerade IT-system lever upp till de föreskrifter som måste beaktas.

Då syftet med att beakta tillämpliga föreskrifter är att de resulterande IT-systemen ska innehålla ändamålsenliga säkerhetsfunktioner bör det finnas en koppling mellan föreskrifter och resultat från hot-, risk- och sårbarhetsanalyserna. Detta kan åstadkommas genom att hot och/eller skyddsåtgärder, och i förlängningen även säkerhetskrav, kopplas till relevanta delar av föreskrifter. Sublime kan då kontrollera att alla identifierade föreskrifter har beaktats i analysen.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.2.2 Förslag på relevanta föreskrifter

Vilka föreskrifter som är relevanta för Försvarsmaktens IT-system förändras kontinuerligt i och med att föreskrifter tillkommer, förändras eller tas bort. Detta gör det svårt att vara uppdaterad på vilka föreskrifter som är aktuella och veta vilka föreskrifter som behöver beaktas vid genomförandet av författnings-analysen.

Som stöd till användaren skulle Sublime kunna ge förslag på relevanta föreskrifter som behöver beaktas. Frågebatteriet skulle exempelvis kunna innehålla frågor angående typ av information, informationsklassning samt systemets omgivning.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.3 Systemskiss

Syftet med att ta fram en systemskiss är att dokumentera vad analysgruppen avser med *IT-systemet* vid genomförandet av analyserna. Då flera personer är inblandade i framtagandet av säkerhetsmålsättningen är det viktigt att alla inblandade har samma bild av det tänkta IT-systemet. Utan en skiss av det tänkta systemet blir det lätt så att mycket tid går åt till diskussioner om vad som avses med IT-systemet och vilka gränsytor det bedöms få.

Framtagandet av säkerhetsmålsättning sker under ett tidigt steg av IT-systems livscykel, vilket medför att en systemskiss bör vara på en generell och

övergripande nivå. Genom framtagandet av en systemskiss måste alltså deltagarna skapa en gemensam bild av det tänkta IT-systemet och dess gränsytor.

Realiseringsförslagen avseende systemskiss presenteras i avsnitt 4.3.1 till 4.3.4. Tabell 4 visar de behov som realiseringsförslagen bedöms kunna tillfredsställa.

Tabell 4: Koppling mellan behov och realiseringsförslag relaterade till systemskiss.

Behov	Bildbilaga	Fri rityta	Skissfunktion med fördefinierade figurer	Gränsytor till verksamheten
Att koordinera analyser för olika IT-system mellan vilka det finns beroenden				X
Att representanter från alla berörda delar av organisationen deltar i analysarbetet				X
Ett arbetssätt som beaktar de hot som är specifika för aktuellt IT-system	X	X	X	X
Ett arbetssätt som kan anpassas så att det står i proportion till IT-systemets omfattning	X	X	X	X
Arbetssätt som tillvaratar tillgänglig information om det planerade IT-systemet	X	X	X	X
Spårbarhet för de antaganden som görs under analyserna	X	X	X	X

4.3.1 Bildbilaga

Deltagarna i analysgruppen har inte alltid samma bild av vad IT-systemet är. Detta kan gälla såväl vad IT-systemet består av samt vilka gränsytor som finns.

För att stödja en gemensam bild skulle Sublime skulle kunna ha stöd för att hantera systemskisser. Skisserna avses konstrueras i extern programvara och importeras i Sublime i form av bilder. Systemskisser skulle utgöra bilagor till analysen och skulle kunna finnas med i det rapportunderlag som presenterar från analysen.

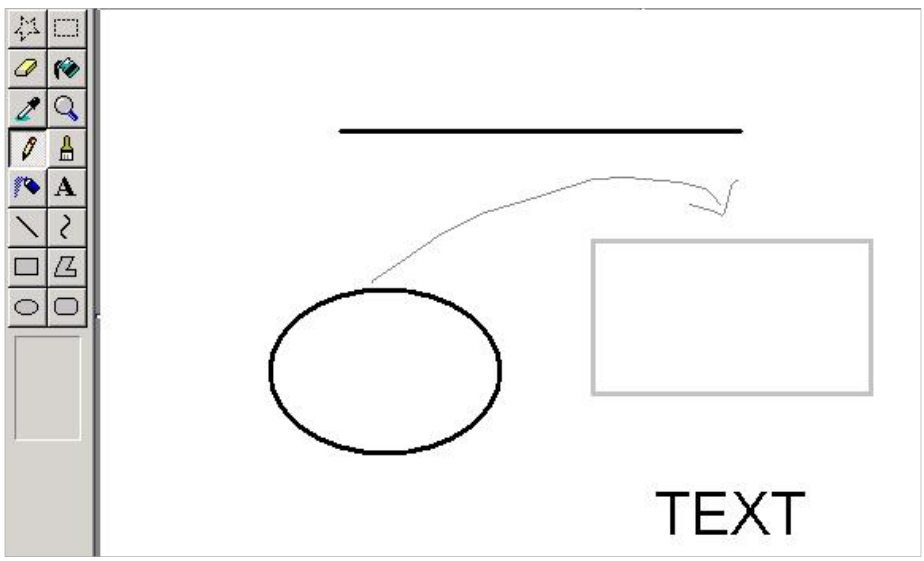
Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.3.2 Fri rityta

Med realiseringsförslaget som återges i 4.3.1 är analysgruppen fortfarande beroende av extern programvara för att skapa systemskisser, vilket inte är optimalt. Möjligheten att genomföra alla delar av analysen i ett och samma program är att föredra.

Möjligheten att skapa systemskisser i Sublime skulle kunna tillgodoses genom att lägga till en rityta där användaren kan skapa en systemskiss. En rityta har enklare funktionalitet där skisser skapas med hjälp av pensel och enklare former såsom linjer, cirklar och rektanglar (Figur 9). Det kan även finnas funktionalitet för att lägga in text i skissen. Den resulterande skissen kan exporteras i något av de vanligare bildformaten som även kan inkluderas i det rapportunderlag som presenterar analysresultaten.



Figur 9: Exempel på en fri rityta.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.3.3 Skissfunktion med fördefinierade figurer

Nackdelar med den fria ritytan som föreslås i 4.3.2 är att det krävs att användaren är bra på att rita för att uppnå en tydlig systemskiss, samt att variationen mellan olika skisser kan bli stor. Med hjälp av en uppsättning fördefinierade figurer skulle framtagandet av systemskisser underlättas och ge mer entydiga resultat.

En lösning med fördefinierade figurer att placera ut på en rityta kräver en uppsättning figurer som motsvarar de flesta behov som kan tänkas uppstå vid framtagning av systemskisser. Ett alternativ kan vara att utgå från en befintlig standard för modellering som exempelvis UML[13].

Beroenden

Detta realiseringsförslag har beroenden till de realiseringsförslag som anges i tabellen nedan.

Tabell 5: Beroenden för realiseringsförslag *Skissfunktion med fördefinierade figurer*.

ID	Namn
4.3.2	Fri rityta

4.3.4 Gränsytor till verksamheten

En viktig aspekt under hot-, risk- och sårbarhetsanalyser för IT-system är vilken verksamhet som det planerade systemet interagerar med, det vill säga IT-systemets gränsytor. Om det finns skisser av det planerade systemet kan de kopplas till den verksamhetbeskrivning som utgör grunden för analyserna. Detta skapar en bra grund för gemensam uppfattning inom analysgruppen såväl som mellan analysgruppen och andra aktörer i auktorisations- och ackrediteringsprocessen. Exempelvis avseende vilka delar av verksamheten som kan påverka eller påverkas av det planerade systemet.

Beroenden

Detta realiseringsförslag har beroenden till de realiseringsförslag som anges i tabellen nedan.

Tabell 6: Beroenden för realiseringsförslag *Gränsytor till verksamheten*.

ID	Namn
4.3.3	Skissfunktion med fördefinierade figurer

[13] http://www.uml.org

4.4 Hotanalys

Hotanalysen genomförs som en del av arbetet med säkerhetsmålsättningen för att identifiera potentiella hot mot planerade IT-system. Syftet med att genomföra en hotanalys är att ta fram den hotbild som utgör underlag vid genomförande av riskanalys.

Realiseringsförslagen avseende hotanalys presenteras i avsnitt 4.4.1 till 4.4.4. Tabell 7 visar de behov som realiseringsförslagen bedöms kunna tillfredsställa.

Tabell 7: Koppling mellan behov och realiseringsförslag relaterade till hotanalys.

Behov	Strukturerad metod för hotanalys	Hotkatalog	Stöd vid värdering av hot	Automatiska förslag på hot
Att analysarbetet genomförs enligt fastställda metoder	X			
Ett arbetssätt som kan anpassas så att det står i proportion till IT-systemets omfattning		X		X
Instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram	X			
Att de antaganden och bedömningar som görs under analysarbetet motiveras				X
Att icke avsiktliga hot beaktas vid genomförandet av hotanalysen	X			X
Spårbarhet för de antaganden som görs under analyserna	X		X	X
Analysresultat som gör det möjligt att bedöma om det planerade IT-systemet kommer att kunna ackrediteras	X		X	X

4.4.1 Strukturerad metod för hotanalys

Att identifiera alla relevanta hot mot ett planerat IT-system är en svår uppgift. En strukturerad metod utgör ett stöd vid identifieringen av hoten. En befintlig sådan metod finns beskriven i kapitel 2 i H SÄK IT Hot[14]. Enligt denna metod identifieras konkreta hot genom att steg för steg ange den information som

[14] Försvarsmakten. (2001). *Handbok för Försvarsmaktens säkerhetstjänst – Informationsteknik hotbeskrivning (H SÄK IT Hot)*. M7745-734051.

efterfrågas. Det konkreta hotet byggs då upp gradvis, istället för att det i ett fritextfält endast efterfrågas en komplett beskrivning av hotet, vilket är fallet i aktuell version av Sublime.

Att svara på kortare frågor gör det enklare att komma igång med analysen samtidigt som det ger ett stöd avseende vilken information som behövs i en hotbeskrivning. En implementation av denna metod innebär att Sublime behöver kompletteras med ett mer detaljerat formulär där användaren kan fylla i den information som efterfrågas enligt metoden i H SÄK IT Hot.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.4.2 Hotkatalog

Dagens hotanalyser utgår i många fall från ett blankt papper alternativt analysgruppsdeltagarnas egenhändigt ihopsatta kataloger över hot. Utformningen av dessa hotkataloger varierar från person till person, vilket gör att även analysresultaten kan variera beroende på vilka personer som deltagit i analysgruppen.

Aktuell version av Sublime innehåller grundläggande funktionalitet för att exportera och importera hot mellan olika analyser. På så sätt är det möjligt att återanvända hotdefinitioner från tidigare genomförda analyser.

Funktionaliteten i Sublime kan utökas för att ge stöd för gemensamma hotkataloger, exempelvis genom att:

- stödja hantering av hotkataloger
- göra det möjligt att välja ut de hot i aktuell katalog som är relevanta för den specifika analysen

Hot från hotkatalogen skulle då motsvara mer generella hot som ofta är relevanta för de vanligaste typerna av IT-system. Hot som är specifika för IT-systemet kan fortfarande definieras separat i analysen utan inblandning av hotkatalogen. Genom att bygga in funktionalitet för hantering av hotkatalog i Sublime skapas förutsättningar för användandet av en gemensam hotkatalog.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.4.3 Stöd vid värdering av hot

Enligt Försvarsmaktens gemensamma riskhanteringsmodell[15] ska alla identifierade hot tilldelas en hotnivå. Inom ramen för Sublime kan stöd för att avgöra de identifierade hotens nivå realiseras genom att en uppsättning frågor besvaras. Dessa frågor kan exempelvis beakta aktörers intention, kapacitet och tillfälle.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.4.4 Automatiska förslag på hot

Oavsett om hotanalysen utgår från en strukturerad metod, en hotkatalog eller både och, baseras den på subjektiva bedömningar av vilka hot som är relevanta att inkludera i hotbilden för det planerade IT-systemet. För att minska behovet av subjektiva bedömningar inom enskilda hotanalyser kan algoritmer som ger förslag på relevanta hot realiseras i Sublime. Verktyget skulle då automatiskt ge förslag på relevanta hot i hotkatalogen utifrån de grundvärden som anges för det planerade IT-systemet i första steget av Försvarsmaktens gemensamma riskhanteringsmodell[15]. De automatiska förslagen på hot kan exempelvis baseras på systemskisser och verksamhetsbeskrivningar.

Med en skissfunktion som utgår från fördefinierade figurer, vilket föreslås i 4.3.3, skulle det kunna vara möjligt att få Sublime att föreslå relevanta hot utifrån den framtagna skissen.

För att uppnå automatiska förslag på hot krävs en tydlig strukturering av information så att det med automatik kan utläsas vad som är vad. Med andra ord betyder det att det krävs inmatningsformulär där användaren svarar på flertalet specifika frågor snarare än att ange en sammanfattning i **ett** fritextfält. Denna typ av formulär är mindre flexibla, men vägleder samtidigt användaren i vilken information som förväntas.

Beroenden

Detta realiseringsförslag har beroenden till de realiseringsförslag som anges i tabellen nedan.

[15] Försvarsmakten. (2009). *Försvarsmaktens gemensamma riskhanteringsmodell*. M7739-350012.

Tabell 8: Beroenden för realiseringsförslag *Automatiska förslag på hot*.

ID	Namn
4.1.1	Strukturerade formulär
4.3.3	Skissfunktion med fördefinierade figurer
4.4.2	Hotkatalog

4.5 Skydd

Med skydd avses den samlade mängden skyddsåtgärder som vidtas för ett planerat IT-system. Syftet med skyddet är att uppnå adekvat IT-säkerhet i IT-systemet. Realiseringsförslagen avseende skydd presenteras i avsnitt 4.5.1 till 4.5.3. Tabell 9 innehåller en överblick av de behov som realiseringsförslagen bedöms kunna tillfredsställa.

Tabell 9: Koppling mellan behov och realiseringsförslag relaterade till skydd.

Behov	Katalog med skyddsåtgärder	Stöd vid val av skyddsåtgärder	Automatiska förslag på skyddsåtgärder
Att analysarbetet genomförs enligt fastställda metoder		X	X
Instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram		X	
Instruktioner och arbetssätt som stämmer överens med varandra		X	
Arbetssätt som tillvaratar tillgänglig information om det planerade IT-systemet		X	X
Spårbarhet för de antaganden som görs under analyserna	X	X	X

4.5.1 Katalog med skyddsåtgärder

Att för varje planerat IT-system börja från början med uppgiften att avgöra vilka skyddsåtgärder som bör införas innebär att tidigare uppbyggd kunskap ej nyttjas. En katalog med skyddsåtgärder kan stödja detta arbete och det finns därför inte behov av att uteslutande förlita sig på den kompetens som finns samlad i

analysgruppen. Tillgång till strukturerad, samlad kunskap om tillgängliga skyddsåtgärder skulle:

- underlätta analysgruppens uppgift
- leda till mer informerade val av skyddsåtgärder
- underlätta kopplingen till hot
- underlätta bedömning av skyddsåtgärders sårbarhetsnivå
- förbättra möjligheterna att återanvända befintliga säkerhetslösningar.

Funktionaliteten i Sublime kan utökas för att ge stöd för fördefinierade kataloger med skyddsåtgärder genom att:

- stödja hantering av kataloger med skyddsåtgärder
- göra det möjligt att välja ut de skyddsåtgärder som är relevanta för den specifika analysen.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.5.2 Stöd vid val av skyddsåtgärder

Identifieringen av relevanta skyddsåtgärder baseras på flera källor, såsom aktuell hotbild, KSF[16] samt resultaten av författnings- och verksamhetsanalyserna. Detta medför att identifieringen av relevanta skyddsåtgärder är en komplex process som måste ta hänsyn till vitt skilda underlag. För att stödja arbetet kan strukturerat metodstöd, som baseras på att användaren besvarar olika delfrågor, utvecklas för att härleda åtgärder från olika källor. En sådan metod kan exempelvis utgöras av ett frågebatteri, vilket realiserar metoden i KSF och därmed avgör vilka delar av KSF som är relevanta för det planerade IT-systemet, samt vidare stöd för att omvandla de erhållna kraven till skyddsåtgärder.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

[16] Försvarsmakten. (2012). *Krav på IT-säkerhetsförmågor hos IT-system v3.0*. HKV 2012-09-24 10 750.64354 Bilaga 1.

4.5.3 Automatiska förslag på skyddsåtgärder

Precis som vid hotanalyser (avsnitt 4.4.4), baseras identifieringen av relevanta skyddsåtgärder utgående från kataloger och strukturerade metoder på subjektiva bedömningar. För att minska behovet av subjektiva bedömningar inom enskilda analyser kan algoritmer som ger förslag på relevanta skyddsåtgärder realiseras i Sublime. De automatiska förslagen på skyddsåtgärder kan baseras på, exempelvis, resultat från författnings- och verksamhetsanalys, systemskiss, hotbild och KSF.

Beroenden

Detta realiseringsförslag har beroenden till de realiseringsförslag som anges i tabellen nedan.

Tabell 10: Beroenden för realiseringsförslag *Automatiska förslag på skyddsåtgärder*.

ID	Namn
4.5.1	Katalog med skyddsåtgärder

4.6 Riskbedömningar

Under riskanalysen ska det göras bedömningar av de identifierade hoten. Det är svårt att göra dessa bedömningar som exempelvis innefattar att bedöma sannolikheter för att olika typer av hot ska realiseras och vilka konsekvenser realiseringen av hot kan medföra.

Realiseringsförslagen avseende riskbedömningar presenteras i avsnitt 4.6.1 till 4.6.2. Tabell 11 innehåller en överblick av de behov som realiseringsförslagen bedöms kunna tillfredsställa.

Tabell 11: Koppling mellan behov och realiseringsförslag relaterade till riskbedömningar.

Behov	Krav på motivering	Bedömningsstöd
Instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram		X
Instruktioner och arbetssätt som stämmer överens med varandra		X

Behov	Krav på motivering	Bedömningsstöd
Arbetssätt som tillvaratar tillgänglig information om det planerade IT-systemet		X
Att de antaganden och bedömningar som görs under analysarbetet motiveras	X	X
Stöd för att avgöra hur implementationen av föreslagna säkerhetskrav påverkar identifierade risker		X
Stöd för att bedöma sannolikhet för realisering av hot		X
Stöd för att bedöma konsekvens vid realisering av hot		X
Spårbarhet för de antaganden som görs under analyserna	X	X
Analysresultat som gör det möjligt att bedöma om det planerade IT-systemet kommer att kunna ackrediteras	X	X
Analysresultat som visar vilka risker som kommer att tas vid användning av det planerade IT-systemet	X	X

4.6.1 Krav på motivering

De bedömningar som görs under riskanalysen kan, vid analystillfället, upplevas som tydliga och självklara för analysgruppen. Dock är det inte alltid lika tydligt för personer utanför analysgruppen på vilka grunder olika bedömningar är gjorda.

I Sublime kan motivering av alla sannolikhetsbedömningar och konsekvensbedömningar krävas. Genom att kräva att bedömningar motiveras måste användaren förklara på vilka grunder dessa bedömningar har gjorts. Ett krav på motivering ger även förbättrad spårbarhet, vilket är till stor nytta då analyser revideras, exempelvis vid omackreditering.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.6.2 Bedömningsstöd

Inom Försvarsmakten finns det i dagsläget finns inget stöd att nyttja när sannolikheter och konsekvenser ska bedömas för konkreta hot mot IT-system. Underrättelseinformation, som exempelvis skulle kunna ge ett bra stöd, är ofta inte tillgängligt för den som ska göra bedömningarna.

Det stöd som finns i dagsläget i Sublime vid bedömning av sannolikheter och konsekvenser är en fastställd sannolikhetsskala, fastställda konsekvensskalor samt ett grafiskt gränssnitt som vid bedömningstillfället presenterar relevant underlag från tidigare steg. Denna funktionalitet erbjuder ett grundläggande stöd, men det är möjligt att ge användaren mer avancerat stöd i processen att komma fram till en rimlig bedömning.

Hotens risknivå utläses från riskmatrisen och baseras på den bedömda sannolikheten och konsekvensen. Istället för att bedöma sannolikhet och konsekvens för varje hot skulle det vara möjligt att endast göra bedömningen för det hot som analysgruppen känner sig mest säkra på. Därefter görs en relativ bedömning av hoten där de jämförs med varandra avseende hur allvarliga de anses vara. Det hot som analysgruppen bedömt sannolikhet och konsekvens för används sedan som referenspunkt för att räkna fram risknivå för de övriga hoten baserat på hotens relativa allvarlighet.

Den relativa bedömningen kan exempelvis göras automatiskt av Sublime baserat på den information som är tillgänglig om hoten. Ett annat alternativ är att låta analysgruppen göra den relativa bedömningen med hjälp av exempelvis AHP[17].

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.7 Säkerhetskrav

Med säkerhetskrav avses de krav som ställs på IT-säkerheten i planerade IT-system. Det har visats att effektiv kravhantering är avgörande för hur väl systemutvecklingsprojekt lyckas[18]. Därför är det viktigt för den fortsatta utvecklingsprocessen att den uppsättning med säkerhetskrav som inkluderas i säkerhetsmålsättningen är tillräcklig för att IT-systemet ska få adekvat IT-säkerhet.

[17] Saaty, T. (1994). *Fundamentals of Decision Making and Priority Theory – with the Analytic Hierarchy Process*, Vol. VI, RWS Publications, Pittsburgh, USA.
[18] N Hallberg, J Haraldsson, N Lewau, J Hansson, H Granlund, T Sundmark, S Nilsson. (2011). *Kravhantering: Best Practise*. FOI-R--3264--SE.

Realiseringsförslagen avseende säkerhetskrav presenteras i avsnitt 4.7.1 till 4.7.2. Tabell 12 innehåller en överblick av de behov som realiseringsförslagen bedöms kunna tillfredsställa.

Tabell 12: Koppling mellan behov och realiseringsförslag relaterade till säkerhetskrav.

Behov	Sammanställning av underlag för säkerhetskrav	Stöd för att formulera säkerhetskrav
Att analysarbetet genomförs enligt fastställda metoder		X
Instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram		X
Instruktioner och arbetssätt som stämmer överens med varandra		X
Arbetssätt som tillvaratar tillgänglig information om det planerade IT-systemet	X	
Spårbarhet för de antaganden som görs under analyserna		X
Analysresultat som gör det möjligt att bedöma om det planerade IT-systemet kommer att kunna ackrediteras	X	X

4.7.1 Sammanställning av underlag för säkerhetskrav

De säkerhetskrav som ska ingå i säkerhetsmålsättningen kan komma från flera olika underlag, exempelvis KSF[19]. Om dessa underlag inte har sammanförts inom ramen för hot-, risk- och sårbarhetsanalysen (så som beskrivs i avsnitt 4.5.2) måste detta göras under framtagandet av säkerhetsmålsättningen. Sublime kan stödja denna sammanställning genom att:

- erbjuda en metod för att avgöra vilka delar av KSF som ska inkluderas
- stödja härledning av krav utgående från resultaten av författningsanalysen samt hot-, risk- och sårbarhetsanalysen

[19] Försvarsmakten. (2012). *Krav på IT-säkerhetsförmågor hos IT-system v3.0*. HKV 2012-09-24 10 750.64354 Bilaga 1.

- generera rapportunderlag baserat på sammanställningen.

Beroenden

Detta realiseringsförslag har beroenden till de realiseringsförslag som anges i tabellen nedan.

Tabell 13: Beroenden för realiseringsförslag *Sammanställning av underlag för säkerhetskrav*.

ID	Namn
4.2.2	Förslag på relevanta

4.7.2 Stöd för att formulera säkerhetskrav

Väl formulerade krav är vitalt för att lyckas utveckla IT-system som är anpassade för den verksamhet och miljö de ska stödja. Tyvärr är de krav som ställs på IT-system ofta bristfälliga. De defekter som återfinns är allt från att krav är otydligt formulerade till att rent av fel krav har specificerats. Användning av strukturerade metoder för att formulera säkerhetskraven kan minska dessa problem.

Grunden för de säkerhetskrav som ska ställas på planerade IT-system erhålls från de skyddsåtgärder som har specificerats inom ramen för analyserna, alternativt från en sammanställning av underlaget för säkerhetskrav (avsnitt 4.7.1). Sublime kan stödja formuleringen av säkerhetskrav genom att realisera den metod som föreslagits av Hansson et al[20].

Beroenden

Detta realiseringsförslag är beroende av att minst ett av de realiseringsförslag som anges i tabellen nedan har realiserats.

Tabell 14: Beroenden för realiseringsförslag *Stöd för att formulera säkerhetskrav*.

ID	Namn
4.5.2	Stöd vid val av skyddsåtgärder
4.5.3	Automatiska förslag på skyddsåtgärder
4.7.1	Sammanställning av underlag för säkerhetskrav

[20] J Hansson, H Granlund, N Hallberg, S Pilemalm, A Pilemalm. (2010). *Kvalitetssäkring vid kravhantering: Granskning av formuleringar*. FOI-R--3070--SE.

4.8 Övrigt

De realiseringsförslag som återfinns under *Övrigt* är förslag som berör alla delar av analyserna. Dessa förslag syftar till att förbättra helhetsintrycket av Sublime genom att tillföra både metodstöd och flexibilitet, samt att förbättra verktygets förmåga att generera rapportunderlag vilket minskar behovet av efterarbete med rapporten. Realiseringsförslagen presenteras i avsnitt 4.8.1 till 4.8.2. Tabell 15 innehåller en överblick av de behov som realiseringsförslagen bedöms kunna tillfredsställa.

Tabell 15: Koppling mellan behov och realiseringsförslag relaterade till alla delar av analyserna.

Behov	Anpassade rapportunderlag	Integration av handböcker
Förståelse för varför analyserna genomförs		X
Engagemang och intresse från ledningen	X	
Att analysarbetet genomförs enligt fastställda metoder		X
Instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram		X
Instruktioner och arbetssätt som stämmer överens med varandra		X
Arbetssätt som tillvaratar tillgänglig information om det planerade IT-systemet	X	
Analysresultat som gör det möjligt att bedöma om det planerade IT-systemet kommer att kunna ackrediteras	X	
Analysresultat som visar vilka risker som kommer att tas vid användning av det planerade IT-systemet	X	

4.8.1 Anpassade rapportunderlag

När analyserna har genomförts finns det ett flertal intressenter av resultaten. De olika intressenterna har dock olika behov avseende vilka delar av analysresultatet som är relevanta för dem. Genom att tillföra funktionalitet för anpassade rapportunderlag skulle Sublime bli mer flexibelt avseende presentation av analysresultat.

En variant av rapportunderlaget kan exempelvis vara anpassat för att motsvara vad som efterfrågas till en säkerhetsmålsättning. En annan variant kan istället ge en inledande sammanfattning (eng. executive summary), vilket skulle vara mer anpassat för de intressenterna som har behov av att snabbt kunna skapa sig en övergripande bild av analysresultaten och det planerade IT-systemet. Ytterligare en variant är rapportunderlag med fokus på spårbarhet. Detta underlag skulle stödja resonemang kring vilka effekter olika förändringar, exempelvis avseende hotbild, verksamhet och skyddsåtgärder, skulle kunna få.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

4.8.2 Integration av handböcker

Inom Försvarsmakten finns det ett stort antal handböcker som beskriver vilka resultat som förväntas produceras vid genomförandet av olika uppgifter. Framtagandet av säkerhetsmålsättningen relaterar till flera olika handböcker och det kan därför upplevas som en svåröverskådlig uppgift.

Sublime skulle kunna stödja användaren genom att relaterade handböcker finns integrerade i verktyget. En integration av handböcker skulle möjliggöra flera olika funktionaliteter, såsom:

- Hjälpknappar i Sublime för att navigera till avsnitt i handböckerna som är relevanta för den specifika uppgift som ska lösas.
- Sökfunktionalitet som gör det möjligt att söka i handböckerna direkt från Sublime.

Beroenden

Detta realiseringsförslag har inga beroenden till övriga realiseringsförslag.

5 Forskningsfrågor

I detta kapitel presenteras ett antal forskningsfrågor som har identifierats under arbetet med att ta fram realiseringsförslag. Jämfört med realiseringsförslagen i kapitel 4 är forskningsfrågorna i detta kapitel inga förslag på lösningar. Genom att studera dessa frågor erhålls kunskap som kan få stor betydelse för utformingen av hot-, risk- och sårbarhetsanalysen samt närliggande arbetsuppgifter och därigenom de säkerhetskrav som ställs på Försvarsmaktens IT-system.

Uppbyggnad av kunskap inom området är väsentligt för att fullt ut kunna tillfredsställa de identifierade behoven avseende stöd vid genomförande av hot-, risk- och sårbarhetsanalyser. För att åstadkomma detta är det nödvändigt att genomföra forskningsstudier.

I följande avsnitt formuleras ett antal väsentliga forskningsfrågor. För att besvara dessa frågor krävs omfattande studier som rör såväl sociala som tekniska frågor. Detta medför behov av omfattande datainsamling för att erhålla kvantitativa såväl som kvalitativa resultat. Ett första steg är att analysera dessa frågor för att avgöra vilken betydelse de olika frågorna har och huruvida de kan besvaras via litteraturstudier eller om de kräver en datainsamling. Möjliga typer av datainsamling är enkäter eller experiment.

5.1 Vad bör en verksamhetsanalys innehålla?

Kunskap om den verksamhet som planerade IT-system ska stödja är en avgörande faktor för förmågan att genomföra hot-, risk- och sårbarhetsanalyser. Resultaten från de verksamhetsanalyser som utgör indata till analyserna är därmed av största vikt. I dagsläget är dock instruktionerna om vad en sådan verksamhetsanalys ska resultera i ytterst vag. Detta kan kompenseras med att kunskap om verksamheten inhämtas från deltagare i de grupper som genomför hot-, risk- och sårbarhetsanalyser istället för ifrån verksamhetsbeskrivningen. En konsekvens av detta är att den verksamhetsanalys som ligger till grund för hot-, risk- och sårbarhetsanalyser kommer att frångås, alternativt modifieras under genomförandet av dessa analyser. Det finns följaktligen flera öppna frågor gällande hur verksamhetanalyser ska genomföras och vilket resultat de ska leverera för att bidra till effektiv hantering av informationssäkerhetsrisker. I kontexten hot-, risk- och sårbarhetsanalys handlar det exempelvis om följande frågor.

- Vilken betydelse har resultaten från verksamhetsanalysen för den följande hot-, risk- och sårbarhetsanalysen, kravställningen av planerade IT-system, systemutvecklingen i stort och Försvarsmaktens samlade informationssäkerhet?

- Vad hos en verksamhet har betydelse för hot-, risk- och sårbarhetsanalyser?
- Hur kan verksamhetens informationssäkerhetsmål utvinnas?
- Vilket underlag krävs för genomförandet av verksamhetsanalyser?
- Vilken betydelse har sammansättningen av analysgruppen och valet av metod för resultatet?

5.2 Förutsättningar för hotanalys

Hotanalyser inom IT-området bygger till stor del fortfarande på någon slags kreativ process där analysdeltagarnas förmåga att identifiera relevanta hot är avgörande. Vid användning av Försvarsmaktens gemensamma riskhanteringsmodell[21] ska hoten även kvantifieras i någon mån. Detta för att förtydliga hotbilden inför riskanalysen.

Det finns dock stora öppna frågor gällande i vilken mån dessa analyser fyller sitt huvudsyfte, det vill säga bidrar till effektiv hantering av informationssäkerhets-risker. I kontexten hot-, risk- och sårbarhetsanalys handlar det exempelvis om följande frågor.

- Vilken betydelse har resultaten från hotanalysen för den följande riskanalysen, kravställningen av planerade IT-system, systemutvecklingen i stort och Försvarsmaktens samlade informationssäkerhet?
- Vilket underlag krävs för att kunna identifiera relevanta hot?
- Vilken betydelse har sammansättningen av analysgruppen och valet av metod för resultatet?

5.3 Förutsättningar för riskbedömning

Enligt gängse metoder bedöms risker genom att sätta värden på sannolikhet och konsekvens kopplad till ett hot. Därefter tas ett riskvärde fram genom att kombinera värdena för sannolikhet och konsekvens. Det finns dock frågetecken gällande huruvida det går att sätta meningsfulla värden. I kontexten hot-, risk- och sårbarhetsanalys handlar det exempelvis om följande frågor.

- Vilken betydelse har resultaten från riskanalysen?
- Vilken precision krävs för att riskvärden ska vara meningsfulla?

[21] Försvarsmakten. (2009). Försvarsmaktens gemensamma riskhanteringsmodell. M7739-350012.

- Vilket underlag krävs för att kunna bestämma riskvärden med nödvändig precision?
- Är det möjligt för en analysgrupp att sätta meningsfulla riskvärden?
- Vilken betydelse har sammansättningen av gruppen och valet av metod för resultatet?

5.4 Automatiserad riskbedömning

Riskanalyser avseende IT-system baseras till stor del på subjektiva bedömningar av sannolikheter och konsekvenser associerade med olika hot. För att minska behovet av subjektiva bedömningar inom enskilda riskanalyser kan algoritmer nyttjas för att genomföra dessa värderingar. Ett verktyg skulle då automatiskt kunna ge förslag på hur risker ska kvantifieras. Riskvärdena kan exempelvis baseras på aktuell hotbild, systemskisser och verksamhetsbeskrivningar.

En automatisering av bedömningen av risker kräver dock att ett antal frågor besvaras.

- Vilka skalor för bedömningen av risker är relevanta för dem som ska nyttja resultaten?
- Vilka faktorer ska tas med i riskbedömningen?
- Vilket underlag krävs för att göra riskbedömningar baserade på de identifierade faktorerna?
- Hur ska sammanvägningen av de olika faktorerna ske?

5.5 Bedömning av precision i de olika analysstegen

Resultaten från hot-, risk- och sårbarhetsanalyser ligger till grund för beslut som påverkar Försvarsmaktens informationssäkerhetsnivå. Samtidigt finns det betydande osäkerheter avseende precisionen hos resultaten från analyserna. Denna osäkerhet bottnar i flera faktorer såsom områdets abstrakta natur, subjektivitet med avseende på värdering av enskilda delar och deras sammanställning. Klargöranden inom detta område kan få stor betydelse för genomförandet av hot-, risk- och sårbarhetsanalyser. Följande frågor utgör exempel på relevanta frågeställningar.

- Hur påverkar osäkerheten i bedömningarna beslutsfattandet?
- Hur kan precisionen i bedömningarna beskrivas på ett meningsfullt sätt?
- Hur kan precisionen hos de enskilda bedömningarna sammanvägas?

- Hur och i vilken mån bör precisionen, eller bristen därav, påverka genomförandet av hot-, risk- och sårbarhetsanalyser?

5.6 Balans mellan nytta och risk

Arbetet med hot-, risk- och sårbarhetsanalyser är fokuserat på de problem som kan uppstå vid införandet av planerade IT-system. En kompletterande aspekt som är viktig att få med i helhetsbedömningarna är vilken nytta planerade IT-system tillför. Detta kan ta sin form i ökad effektivitet i verksamheten. Då IT-system ofta ersätter andra system eller manuell hantering av information kan de dock även minska verksamheters övriga informationssäkerhetsrisker. Hur balansen mellan nytta och risk ska kunna beaktas inom ramen för hot-, risk- och sårbarhetsanalyser leder till ett antal frågeställningar.

- Hur kan information om nyttan med planerade IT-system konkretiseras inom ramen för hot-, risk- och sårbarhetsanalyser?
- Hur kan planerade IT-systems positiva påverkan på verksamheters informationssäkerhet kvantifieras?

6 Slutsatser

Det finns en demonstrator (Sublime) framtagen av FOI i samarbete med FMKE vilken stödjer analysarbete som genomförs enligt Försvarsmaktens gemensamma riskhanteringsmodell. Sublime är utformad så att den även kan testas i samband med genomförande av hot-, risk- och sårbarhetsanalyser. Inom ramen för samarbetet med FMKE planeras ett användningstest att genomföras under december. Fler användningstest planeras att genomföras inom ramen för FoT-projektet under första kvartalet 2013. Målet är att Sublime även ska utvärderas inom ramen för ordinarie analysarbete.

De förslag till utveckling av Sublime som presenteras i denna rapport relaterar framförallt till genomförandet av hot-, risk- och sårbarhetsanalyser. Vissa förslag relaterar även till angränsande aktiviterer såsom verksamhetsanalys och formulering av säkerhetskrav. Utvecklat stöd för genomförande av dessa aktiviter är viktigt såväl för att det ska finnas adekvat underlag för genomförande av hot-, risk- och sårbarhetsanalyser som för att resultaten från dessa analyser ska få full effekt på det fortsatta arbetet i IT-livscykeln.

Ett grundläggande antagande är att många av de behov användarna har avseende hot-, risk- och sårbarhetsanalyser kan tillfredsställas genom införande av ändamålsenliga strukturerade metoder med tillhörande verktygsstöd. Målet är att utvecklad version av Sublime under 2013 ska visa huruvida konceptet fungerar och därmed stödjer mer systematiskt och effektivt arbete med hot-, risk- och sårbarhetsanalyser för Försvarsmaktens IT-system. På längre sikt är målet att den uppbyggda kunskapen ska överföras till Försvarsmakten genom verktygsstöd och metodik. Avseende verktyg kan det handla om faktiskt framtagande eller stöd i olika form vid utveckling av verktygsstöd, exempelvis under kravställning och upphandling.

Parallellt med realiseringsförslagen har ett antal forskningsfrågor identifierats. Resultaten från studier baserade på dessa frågor kan få stor inverkan på synen på hot-, risk- och sårbarhetsanalyser och deras genomförande.

7 Fortsatt arbete

Forskningsprojektet *Effektivare hot-, risk- och sårbarhetsanalyser* kommer under 2013 framförallt att fokusera på de realiseringsförslag som presenterats i kapitel 4. Målsättningen är att i kvartal fyra 2013 kunna leverera en demonstrator till Försvarsmakten som tillfredsställer en betydande delmängd av de behov av stöd som återges i kapitel 3. De föreslagna realiseringsförslagen bedöms vara av en sådan omfattning att de, var för sig, bör vara möjliga att genomföra inom ramen för arbetet under 2013.

Förslagens omfattning varierar stort och för flertalet förslag finns det beroenden som påverkar vad som är möjligt att uppnå. Den inmatade informationens kvalitet och struktur sätter i många fall ribban för vad som är möjligt att uppnå. Exempelvis påverkar informationens struktur till hög grad möjligheterna till automatisering. Därför utgör de realiseringsförslag som relaterar till inmatning av information i Sublime en grundförutsättning för flera av de övriga förslagen.

Forskningsfrågorna i kapitel 5 hamnar lätt i skymundan då fokus för 2013 först och främst ligger på de konkreta realiseringsförslagen. Frågorna lyfter fram flertalet viktiga frågeställningar som kan leda till stora framsteg inom arbetet med hot-, risk- och sårbarhetsanalyser inom Försvarsmakten. Frågeställningarna bör beaktas av kommande projekt och det fortsatta arbetet inom området.

Nästa steg, inom ramen för projektet, är att prioritera realiseringsförslagen och ta fram den ordning i vilken de bör realiseras för att uppnå största möjliga effekt med de resurser som finns tillgängliga. Därefter påbörjas realiseringen av den demonstrator som ska levereras till Försvarsmakten i slutet av 2013.