Erfarenheter från utveckling och förvaltning av IT-system

HENRIK KARLZÉN, DANIEL EIDENSKOG, JACOB LÖFVENBERG

FOI-R--4423--SE
ISSN 1650-1942 April 2017

Henrik Karlzén, Daniel Eidenskog,
Jacob Löfvenberg

Erfarenheter från utveckling och förvaltning av IT-system

Titel	Erfarenheter från utveckling och förvaltning av IT-system
Title	Experiences of development and maintenance of IT systems
Rapportnr/Report no	FOI-R--4423--SE
Månad/Month	April
Utgivningsår/Year	2017
Antal sidor/Pages	36
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E72677
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Informationssäkerhet kan upplevas som ett hinder vid utveckling och användning av IT-system. När det gäller system med särskilt höga krav på IT-säkerhet blir säkerhetsåtgärderna omfattande, vilket medför ett omfattande arbete innan ett system är ackrediterat och får användas i verksamheten. Denna rapport presenterar en intervjustudie avseende erfarenheter av säkerhetsarbete relaterat till IT-system för hantering av information som omfattas av försvarssekretess. Respondenterna arbetar med frågor relaterade till IT-säkerhet hos Försvarsmakten, civila myndigheter och näringslivet. Deras samlade erfarenhet omfattar teknik och processer under utveckling, ackreditering och drift. Intervjusvaren har analyserats ur två perspektiv för att brett belysa området.

Respondenterna ger en bild av att det finns många utmaningar i strävan mot det ideala men ouppnåeliga målet med absolut säkerhet. Systemen ökar i komplexitet, vilket gör ackrediteringsprocessen allt mer krävande. Dessutom ökar kommunikationen mellan IT-system vilket ger högre exponering mot angrepp. Ett överdrivet fokus på säkerhet kan leda till system som kräver mer tid och pengar att ta fram, samtidigt som nya arkitekturer och funktioner uteblir. Respondenterna är i stora drag överens om att det nuvarande tankesättet behöver justeras så att fokus hamnar på ett kontinuerligt och aktivt säkerhetsarbete under hela systemets livslängd, med en utvidgning från enbart teknisk säkerhet. En viss förändring av synen på risk har redan introducerats i Försvarsmakten men fortfarande verkar yttranden om säkerhet tolkas absolut utan att väga in verksamhetsnyttan.

En slutsats är att det skulle vara värdefullt att utreda hur IT-säkerhetsaspekter och ackreditering ska hanteras i Försvarsmakten för att bättre kunna tillgodose verksamhetens behov i framtiden.

Nyckelord: Informationssäkerhet, ackreditering, IT-arkitektur, IT-säkerhet, riskhantering, riskbaserad säkerhet

Summary

Information security can be perceived as a hindrance to the development and usage of IT systems. Regarding systems with particularly high demands on IT security the protective measures are extensive, requiring a lot of work to get the system accredited and approved. This report presents an interview study with a focus on experiences of working with security regarding IT systems that handle information of national security concern. The respondents' work encompass IT security in the Swedish Armed Forces, civilian government agencies, and the business sector. Their collective experience entails technology and processes during development, accreditation and maintenance. Their responses are analysed in two ways in order to effectively describe the problem area.

The respondents' view is that there are many challenges in reaching the ideal, but unreachable, goal of absolute security. Systems are increasingly complex, making the accreditation process more demanding. Excessive security focus may lead to systems that demand more time and financial resources to develop, while new architectures and features remain absent. The respondents generally agree that the current way of thinking needs to be adjusted so that focus is shifted to a continuous and active security process for the entire IT system life span and a broadening from merely technical security. A certain change in how risk is viewed has already been introduced in the Armed Forces but statements on security still seem to be interpreted in an absolute way without taking operational needs into account.

A conclusion is that it would be valuable to investigate how IT security and accreditation should be handled in the Armed Forces to better meet operational needs in the future.

Keywords: Information security, accreditation, IT architecture, IT security, risk management, risk based security

Innehållsförteckning

1 Inledning

Personer i Försvarsmakten och relaterade organisationer framför ibland uppfattningar om att IT-processen och ackrediteringsprocessen är besvärlig och att modernt IT-stöd inte får tillräckligt genomslag inom Försvarsmakten. Ju högre informationssäkerhetsklass IT-systemen ska hantera, desto vanligare verkar uppfattningarna vara.

Om dessa uppfattningar är förankrade i verkliga problem finns det skäl att undersöka dem noggrannare för att bättre förstå och i möjligaste mån hantera dem. Ett första steg är att förtydliga bilden av vilka åsikter som finns. Denna bild kan sedan ligga till grund för vidare arbete med att identifiera vilka åsikter som går att relatera till specifika problem som kan åtgärdas och vilka som måste accepteras. Givet dessa utgångspunkter är frågan som denna studie har behandlat:

Vilka uppfattningar finns som relaterar till Försvarsmaktens IT- process – särskilt med avseende på IT-system med hög informationssäkerhetsklass?

Studien har baserats på intervjuer med individer som innehar olika roller relaterade till utveckling och förvaltning av Försvarsmaktens IT-system. Respondenterna hade som grupp god insikt i hur Försvarsmakten arbetar med IT-frågor, både vad gäller utveckling och förvaltning. Resultatet av intervjuerna har analyserats ur två perspektiv i syfte att identifiera och belysa gemensamma teman bland de uppfattningar som erhölls i intervjusvaren.

Denna studie tangerar delar av innehållet i flera tidigare FOI-rapporter[1] där personer med stor kunskap om Försvarsmaktens IT-utveckling intervjuats. I dessa har syftet dock varit att besvara specifika frågeställningar avseende Försvarsmaktens IT-utveckling. Studien som presenteras i denna rapport är istället explorativ till sin natur och syftar till att skapa en bred bild av de uppfattningar som finns. FOI har stor erfarenhet av IT-säkerhetsforskning riktat mot Försvarsmaktens behov. Detta har gett en omfattande förförståelse för de problem som finns inom området, något som tillåtits vara vägledande i analysen av det insamlade materialet och vid tolkningen av resultatet.

Den resterande delen av rapporten inleds med en beskrivning av studiens metod i kapitel 2. Kapitel 3 och 4 utgör presentationer av respondenternas svar utifrån två analysperspektiv. Det första perspektivet presenteras i kapitel 3 och utgår från de grundfrågor som beskrivs i avsnitt 2.1.2. Det andra perspektivet baseras på ett antal identifierade kategorier och presenteras i kapitel 4. I kapitel 5 beskrivs studiens resultat och rapporten avslutas i kapitel 6 med författarnas diskussion.

[1] Se till exempel Hallberg, Bengtsson och Sommestad, *Effektivare hot-, risk- och sårbarhets-analyser*, FOI-R--3785--SE och de FOI-publikationer som pekas ut i den rapportens Kapitel 1.

2 Metod

Den utgångspunkt som beskrevs i kapitel 1 är relativt allmän hållen och är av tydligt kvalitativ karaktär. Studien har inte undersökt hur utveckling och förvaltning av IT-system i Försvarsmakten faktiskt går till. Syftet har istället varit att belysa och formulera de uppfattningar som finns om Försvarsmaktens utveckling och förvaltning av IT hos personer med god insikt i detta.

För att undersöka vilka uppfattningar som finns genomfördes kvalitativa intervjuer i semistrukturerad form. Intervjuer är ett sätt att skapa kunskap i samspel med respondenterna genom att samla in och tolka deras uppfattning om världen (Kvale 1997).

2.1 Intervjuer

Semistrukturerade intervjuer är en vanlig metod för genomförandet av kvalitativa studier. Metoden är lämplig att använda när det är respondentens uppfattningar som söks, snarare än rena faktauppgifter. Eftersom semistrukturerade intervjuer rör sig relativt fritt inom det område som intervjuaren undersöker tillåts respondenten en större frihet att följa sina egna associationer och tankebanor än vid en mer styrd intervju.

Valet av respondenter gjordes för att stödja det explorativa syftet med studien. Detta innebar att respondenterna valdes från flera olika organisationer och flera olika roller. Detta för att så snabbt som möjligt nå ”mättnad” i datainsamlingen, dvs. nå den punkt när ytterligare datainsamling inte längre tillför något nytt. Detta stämmer väl med synen hos Strauss och Corbin (1998, s. 292) som hävdar att datainsamlingen bör fortsätta ”until theoretical saturation takes place [...] Any new data would only add, in a minor way, to the many variations of major patterns”.

Antalet respondenter ska vara stort nog för att ”mätta” datainsamlingen, men blir antalet för stort blir en noggrann tolkning av intervjuerna omöjlig (Kvale 1997). I ett försök att balansera dessa två motstridiga egenskaper användes sjutton respondenter. Detta gav ett datamaterial som i omfattning inte var ohanterligt stort samtidigt som det fanns påtagligt överlapp i respondenternas uppfattningar, vilket kan tolkas som tecken på den mättnad som önskas i datainsamlingen.

2.1.1 Intervjufrågor

Åtta grundfrågor formulerades som utgångspunkt för intervjuerna. Eftersom studien var explorativ till sin karaktär var frågorna inte formulerade för att direkt kunna användas vid intervjuerna. Avsikten var istället att översiktligt ringa in det

område som studien önskade röra sig inom, och efter vidare bearbetning utgöra underlag för de semistrukturerade intervjuerna.

Grundfrågor

1. Hur har den generella IT-utvecklingen påverkat verksamhetens och användarnas förväntningar och acceptans för IT-system byggda efter Försvarsmaktens krav på informations- och IT-säkerhet?
2. Hur har utvecklingen vad gäller hotbild och motmedel sett ut?
3. Hur har synen på risker och därmed riskhanteringen ändrats över tiden för Försvarsmaktens IT-system?
4. Hur har sättet att värdera information ändrats över tiden, exempelvis vid sekretessklassificering?
5. Hur har synen på assurans ändrats över tiden i utveckling och granskning av Försvarsmaktens IT-system?
6. Hur har synen på riskavvägningar och assurans utvecklats i andra länder?
7. Hur har byggsätt, till exempel arkitektur och komponenter, ändrats över tiden?
8. Hur är synen på färdiga byggstenar såsom COTS, öppen/sluten källkod och liknande?

Utgående från grundfrågorna utformades mer konkreta intervjufrågor för att göra det enklare för respondenterna att svara. Intervjufrågorna hölls på en relativt öppen nivå för att undvika att svaren färgades av intervjuaren samt för att passa studiens explorativa natur, där bredden på respondenternas svar var svår att förutsäga. Intervjufrågorna återfinns i sin helhet i Appendix A.

2.1.2 Intervjugenomförande

För att säkerställa att intervjumaterialet höll hög kvalitet och var förhållandevis enkelt att bearbeta efter intervjuerna lades relativt stort arbete ner på att planera och utforma intervjuerna. Till exempel genomfördes en FOI-intern workshop där en forskningschef som inte ingick i studien, men som har stor erfarenhet av intervjustudier, stödde studiegruppen i planeringen och utformningen av intervjuerna. Dessutom genomfördes en provintervju med en FOI-forskare inom IT-säkerhetsområdet för att testa intervjutid och frågeutformning.

Två forskare höll gemensamt i intervjuerna, där en forskare främst förde anteckningar medan den andra forskaren ställde frågor och höll i gång diskussionen. Den som antecknade kom i vissa fall med följdfrågor efter att den huvudsaklige frågeställaren var färdig med ett frågeavsnitt och kunde också vid behov påpeka om diskussionen hamnat utanför studiens intresseområde.

Vid genomförandet av intervjuerna lades vikt vid att respondenterna skulle känna sig bekväma i situationen och att så många som möjligt av deras uppfattningar

skulle komma fram och dokumenteras på ett korrekt sätt. Ingen transkribering av intervjuerna gjordes dock. Det bedömdes att det skulle vara allt för tidskrävande givet ramarna för studiens genomförande.

Efter intervjuerna renskrevs anteckningarna. Närvaron av två personer vid intervjuerna gav goda möjligheter att fånga det som respondenterna uttryckt under intervjuerna. I de fall det fanns tveksamheter i hur svaren skulle tolkas kontaktades respondenterna igen för att klargöra deras svar.

Respondenternas roll lyste ofta igenom i svaren genom att en viss synvinkel togs. En tekniker var till exempel mer benägen att lösa problem med teknik, en företagsrepresentant var mer benägen att sälja sina produkter och en myndighetsperson ville gärna att dennes specifika ansvarsområde skulle få ökat fokus. Detta har inte hanterats på något särskilt sätt utan har betraktats som en naturlig variation i form och innehåll hos svaren från respondenterna.

2.2 Analys

De renskrivna intervjuanteckningarna från de genomförda intervjuerna utgjorde det datamaterial som användes för analysen. Materialet bestod av ett relativt stort antal utsagor relaterade till intervjufrågorna. Ett sådant material måste analyseras för att teman och tendenser i innehållet ska bli synliga. Analysen gjordes i tre steg:

1. Bestäm kategorier.
2. För varje utsaga i datamaterialet, placera utsagan i den eller de kategorier där den passar.
3. Beskriv varje kategori.

2.2.1 Kategorival

Valet av kategorier bestämmer vilket perspektiv som läggs på datamaterialet och olika val av kategorier lyfter fram olika egenskaper. För att utnyttja materialet så effektivt som möjligt gjordes två olika kategoriindelningar, vilket resulterade i två olika analyser som redovisas i var sitt kapitel. De två alternativa kategoriindelningarna beskrivs nedan.

Kategoriindelning baserad på grundfrågorna

Grundfrågorna var utgångspunkten för hela intervjuserien varför de sågs som en naturlig kategoriindelning. Datamaterialet analyserades och utsagorna sorterades, när så var möjligt, efter dessa kategorier.

Kategoriindelning baserad på datamaterialet

För att bättre fånga uppfattningar som inte naturligt passar in under någon av grundfrågorna gjordes en analys utan i förväg formulerade kategorier. Analysen

använde väsentligen samma steg som *grundad teori*[2] (Strauss och Corbin 1998) men med skillnaden att datainsamlingen i detta fall i sin helhet gjordes innan analysen, snarare än iterativt, parallellt med analysen.

2.2.2 Sortering av utsagor

Sorteringen har gjorts genom att lägga varje utsaga till de kategorier där den passade. I fallet med kategorival med utgångspunkt från datamaterialet formulerades kategorierna inte explicit förrän i efterhand varför kategorierna var preliminära och föränderliga under sorteringsfasen.

2.2.3 Beskrivning av kategorier

Efter sorteringen av utsagor fanns ett relativt stort textmaterial i varje kategori. Det var allt för stort för att återges i sin helhet och allt för varierande i form, stil och nivå för att på ett bra sätt återges i löpande text. Som en del i analysarbetet har studiegruppen därför, utgående från sin erfarenhet inom området, tolkat utsagorna och formulerat sammanfattande beskrivningar för varje kategori. Detta har gjorts baserat på ord och fraser från utsagorna för att fånga stilen och känslan i datamaterialet.

2.3 Respondenter

Respondenternas roll, kunskapsnivå och organisationstillhörighet varierade. En del respondenter hade en mer teknisk bakgrund och roll medan andra var på en mer övergripande, verksamhetsorienterad nivå.

Respondenterna hade domänkompetens inom områdena IT-arkitektur och informationssäkerhet i allmänhet. Dessutom hade de kunskap om kravbilden för IT-säkerhet inom Försvarsmakten eller motsvarande utländska organisationer. Flera av respondenterna hade även förståelse för militär verksamhet, exempelvis genom att de var officerare.

Sex intervjuer gjordes inom myndighetsvärlden, fördelade på tre myndigheter (varav en var Försvarsmakten) och totalt tio personer. Fem intervjuer gjordes inom näringslivet, fördelade på fyra företag och totalt sju personer. De totalt elva intervjuerna finns översiktligt sammanställda i tabell 1 nedan.

[2] Grundad teori (eng. grounded theory) är en metod för att analysera kvalitativt datamaterial utan att ha en kategoriindelning i förväg. Analys med grundad teori kan kort beskrivas som att data som uppfattas som likartad läggs samman till grupper som efter hand blir allt större. Grupperna namnges och tillsammans med deras inbördes relationer bildar de det som kallas en teori som på ett effektivt sätt beskriver det undersökta fenomenet.

Tabell 1. Respondenter per intervju och organisation.

Intervju	Organisation	Antal respondenter
1	Företag A	2
2	Företag B	2
3	Företag C	1
4	Företag D	1
5	Företag D	1
6	Myndighet P	4
7	Myndighet Q	2
8	Försvarsmakten	1
9	Försvarsmakten	1
10	Försvarsmakten	1
11	Försvarsmakten	1
	Totalt	17

2.4 Metodanalys

Studien som presenteras i denna rapport har utgått från ett antal grundfrågor och genomfördes som en serie av semistrukturerade intervjuer med tillhörande analys. Grundfrågorna var inte möjliga att använda direkt i intervjuerna då dessa ansågs vara på en allt för abstrakt och övergripande nivå. Inför intervjuerna konkretiserades grundfrågorna därför till intervjufrågor. I den mån vissa grundfrågor endast delvis kunde belysas berodde det i huvudsak på att svaren på intervjufrågorna var knapphändiga inom dessa områden. Det är möjligt att andra intervjufrågor hade medfört att respondenterna uttalat sig även kring dessa aspekter i grundfrågorna, men då sannolikt till kostnaden av minskad omfattning av diskussionen relaterad till de frågor som faktiskt användes. Givet studiens ramar anser författarna därför att det insamlade materialet ger en god bild av området som helhet.

Tidigt i studien genomfördes en testintervju med en av studiens medlemmar och de svar som gavs i den intervjun stämde relativt väl med de svar som sedan framkom i de riktiga intervjuerna. Detta indikerar att de åsikter som gavs av respondenterna även återfinns utanför den utvalda gruppen.

Inom respondentgruppen fanns en spridning i svaren. Bland annat avspeglades respondenternas huvudsakliga arbetsuppgifter, bakgrundskunskap och intressen så till vida att dessa områden fick störst fokus i respektive intervju. Detta tyder på att det var respektive respondents egen åsikt som framfördes och inte en inlärd, officiell beskrivning som återgavs.

Den information som samlades in från respondenterna utgjordes av deras uttalanden under intervjuerna utan att noteringar gjordes gällande icke-verbal kommunikation som till exempel intonation, tveksamhet, kroppsspråk eller annat som kunde ha visat på om respondenten egentligen ansåg något annat än vad som uttrycktes verbalt. Den icke-verbala kommunikationen användes dock som indata under intervjuerna för att exempelvis identifiera om det fanns möjlighet att utveckla ett svar vidare eller ta upp andra perspektiv på en fråga. Författarna anser att denna begränsning av informationsinhämtningen är acceptabel i studien då endast konkreta och primärt tekniska frågor har diskuterats snarare än till exempel personligt känsliga ämnen.

3 Analys utifrån grundfrågorna

I analysen som ligger till grund för detta kapitel har respondenternas utsagor sorterats utifrån grundfrågorna i avsnitt 2.1.1. Utsagorna har därefter tolkats och sammanfattats i löpande text. Detta har gjorts baserat på ord och fraser från utsagorna för att fånga stilen och känslan i datamaterialet. Ingen ytterligare bearbetning har gjorts, utan den löpande texten under varje grundfråga beskriver de insamlade utsagorna på ett så källtroget sätt som möjligt.

3.1 Grundfråga 1

Hur har den generella IT-utvecklingen påverkat verksamhetens och användarnas förväntningar och acceptans för IT-system byggda efter Försvarsmaktens krav på informations- och IT-säkerhet?

Traditionellt har det inom Försvarsmakten varit ett betydande fokus på sekretess som säkerhetsegenskap medan riktighet och framförallt tillgänglighet fått stå tillbaka. Ofta upplevs det inte bara finnas olika fokus, utan när det gäller att upprätthålla en egenskap så verkar det ske på bekostnad av en annan egenskap. Till exempel är backuper ett bra sätt att förbättra tillgängligheten, men sekretessen hotas eftersom informationen nu finns på flera ställen. Samtidigt framhöll en del respondenter att många av de funktioner som skyddar sekretessen också ger positiva bieffekter på tillgänglighet och riktighet, exempelvis när det gäller intrångsskydd.

När det gäller integration av system ger ökad prestanda och framförallt större beräkningskraft nya möjligheter att behandla stora mängder data vilket kan göra centralisering av databehandling mer attraktivt. Integration för dock med sig vissa utmaningar eftersom antalet berörda system ökar. Systemen kravställs vanligtvis var för sig vilket gör det oklart vem som ska hantera de krav som uppstår i samband med integrationen.

Utöver tillgänglighet kommer även riktighet som säkerhetsegenskap ofta i skymundan. I den generella IT-utvecklingen syns riktighet som en allt viktigare egenskap. Framförallt kommer inspiration från sjukhusmiljöer samt industriella informations- och styrsystem (eng. SCADA). Riktighet i vidare bemärkelse inkluderar att informationen faktiskt är korrekt och inte missvisande. Även riktighetsaspekten har fått mer fokus i den generella utvecklingen, men det är oklart om denna utveckling fått någon praktisk påverkan på Försvarsmakten och dess krav på säkerhet. En möjlighet är att verksamheten påverkas i varierande grad beroende på hur tidskritisk den är.

3.2 Grundfråga 2

Hur har utvecklingen vad gäller hotbild och motmedel sett ut?

Intervjuerna indikerar att de senaste 15 åren gett en utveckling mot verktyg som automatiserar både IT-angrepp och IT-försvar. Dessutom har en marknad för att köpa och sälja information om säkerhetshål vuxit fram. Sammantaget gör detta att den tekniska kompetensen på sätt och vis står mindre i fokus även om riktiga specialister kan vara mer värdefulla för att verkligen gå på djupet. Samtidigt har det generellt sett, och även till viss del i Försvarsmakten, insetts att allt inte går att lösa med teknik. Användarna och insiderproblematiken har fått många rubriker och säkerhetsmedvetandet har ökat. Flera respondenter beskriver ett behov av rolluppdelning och flerhandsfattning för att hantera hot från insiders. Erfarenhets- eller relationsbaserad åtkomstkontroll är andra sätt att tala om problematiken och dess möjliga lösningar.

Hotaktörerna har gått från att främst vara enskilda intresserade till att allt oftare vara statsmakter och organiserad brottslighet. På samma sätt har ett intresse vuxit fram för att som försvarare samordna sig till större strukturer. Även om samarbete kring skydd upplevs vara lämpligt är det en utmaning att dela information om den specifika hotbilden med andra.

På sätt och vis finns en asymmetri i IT-krigföringen eftersom angriparen bara behöver hitta ett enda säkerhetshål medan den försvarande sidan måste täppa till samtliga hål som angriparen kan tänkas använda – oftast utan att veta vilka hål som kommer att utnyttjas. Å andra sidan kan den som hittar eller träffas av ett cybervapen relativt enkelt studera, förändra och återanvända vapnet. Det är svårt att veta om statsmakter och andra aktörer begränsar sina offensiva aktiviteter på grund av denna risk. Asymmetrin gäller även kryptografiska skydd som måste hålla en särskilt lång tid då inhämtad information kan ligga i vila hos angriparen till dess att tillräckligt kraftfulla beräkningsresurser och angreppsmetoder tagits fram.

3.3 Grundfråga 3

Hur har synen på risker och därmed riskhanteringen ändrats över tiden för Försvarsmaktens IT-system?

Även om säkerhetsmålsättningar och säkerhetskrav fått större acceptans och blivit mer etablerade i Försvarsmaktens verksamhet under de senaste 15 åren så upplevs det som att det finns alltför stor tyngdpunkt på dessa krav snarare än verksamhetens behov. Absolut säkerhet, framför allt avseende sekretess, upplevs driva IT-säkerhetsarbetet på bekostnad av verksamhetsnyttan. Det måste finnas metoder för att göra en aktiv avvägning mellan sekretess och tillgänglighet, särskilt för nödsituationer.

Generellt medför den ökade komplexiteten att det blir svårare att veta vad systemet består av och därmed hur det ska säkras. Den ökade integrationen mellan system ger samtidigt större exponering. Som följd av detta framkom i intervjusvaren en ovisshet om det fortfarande går att säkra på systemnivå eller om det är bättre att försöka säkra informationsobjekt. Komplexiteten medför även att det blir allt fler delar att säkra. Det faktum att systemet och dess information kan ha olika livslängd spelar även roll.

För att kompensera för den rådande strävan mot absolut säkerhet, föreslog flera respondenter att en helhetsbild avseende riskhantering behövs kombinerat med styrning och ledarskap. I dagsläget kan det vara svårt att samla alla intressenter vid en riskanalys och kanske framförallt att få dem att förstå varandra. Riskanalyser upplevs generellt som svåra att genomföra. En faktor kan vara att informationshanteringsreglerna sällan är anpassade för IT-system. Exempelvis är det svårt att förhålla sig till lagar som rör handlingar och uppgifter när IT-systemen snarare innehåller datamängder och informationsobjekt. Ett tydligare ledarskap skulle dock kunna öppna för att göra genomtänkta avsteg från reglerna och den absoluta, förebyggande säkerheten och istället satsa på riskhantering och detektering. Detta skulle i sin tur skapa möjligheter för bättre tillgänglighet och verksamhetsnytta.

Absolut säkerhetstänk och kravfokus ger också ett granskningsfokus, där produkter och lösningar kontrolleras på ett omfattande sätt. En sådan granskningsprocess kan leda till flera års fördröjningar och en ovisshet om huruvida systemet överhuvudtaget kommer att godkännas och i så fall när. I praktiken tröttas ofta granskare ut av lösningar som utgörs av lapptäcken där en ny del sätts på efter varje granskningsavslag. *Krav på IT-säkerhetsförmågor hos IT-system v3.0 – KSF3* (Försvarsmakten, 2012) hade enligt flera respondenter en god grundidé med mindre fokus på absolut teoretisk säkerhet oberoende av omständigheterna, för att istället lyfta fram exponering som viktig faktor. Dessutom verkar KSF3 vara ett försök att göra det lättare att realisera kraven genom att ge förslag på lösningar, ungefär på samma sätt som Common Criteria gör. Dock upplevs inte KSF3 ha fått genomslag på dessa punkter.

En annan granskningsaspekt som framkom i intervjuerna är att det finns en oro att separationen mellan kravställare och granskare är undermålig då det är samma del av organisationen som står för båda uppgifterna. Vidare verkar det absoluta säkerhetstänket leda till en ackreditering som utgörs av ett engångssteg snarare än en del av en kontinuerlig livscykelprocess. System förändras över tiden och då måste säkerheten hänga med. När ett säkerhetshål upptäcks måste en avvägning göras mellan att introducera en patch, som kanske inte går att lita på kvalitets- och säkerhetsmässigt, och att låta säkerhetshålet bestå. Andra säkerhetsmekanismer som bidrar till säkerheten över tid är bland annat penetrationstestning samt aktiv övervakning och logganalys för att hantera insiders.

3.4 Grundfråga 4

Hur har sättet att värdera information ändrats över tiden, exempelvis vid sekretessklassificering?

Respondenterna lyfter fram att en stor fördel med IT-system är möjligheten att samla och analysera stora mängder information. För att inte begränsa dessa möjligheter vore det fördelaktigt att i ett och samma IT-system kunna blanda information med olika informationssäkerhetsklass. Detta ökar dock vissa risker. Även om olika informationsobjekt inte har så hög sekretessklassificering var för sig kan aggregatet ge upphov till ett högre skyddsvärde. Vidare ska användare i Försvarsmakten enbart ha tillgång till den information som användaren faktiskt har legitim nytta av. Därmed bör tillgången inte nödvändigtvis begränsas per informationssäkerhetsklass utan snarare på exempelvis projektnivå eller till och med per informationsobjekt.

För att tillgången till information ska kunna styras per objekt vore det lämpligt om de olika informationsobjekten kunde märkas var för sig. Det kan dock vara svårt att få en dylik märkning att vara tillräckligt hårt knutet till objektet samtidigt som det tar tid att märka och därmed klassificera informationsobjekt. Alltför mödosamt säkerhetsarbete leder till att verksamhetsnyttan snarare begränsas än ökar på grund av informationsaggregaten. En risk är också att användare nyttjar genvägar, till exempel genom att slentrianmässigt klassa information på en hög nivå för att inte råka klassa någon information för lågt.

För högre informationssäkerhetsklasser pekar flera respondenter på att det är troligt att informationen ändras mer sällan än på lägre nivåer. Detta gör att klassificering och hantering blir mindre betungande åtminstone på dessa nivåer.

Spårbarhet komplicerar klassificeringen av informationsobjekt över tiden. Om viss information inte längre behöver hemlighållas för sin egen skull kan det vara önskvärt att klassificera ned informationen. Men loggar som förhåller sig till tidigare användning av informationen kan även fortsatt behöva behållas i den högre informationssäkerhetsklassen, vilket även kan påverka grundinformationen. Av denna anledning kan informationens säkerhetsklassning behöva bibehållas trots att informationens sekretess spelat ut sin roll.

3.5 Grundfråga 5

Hur har synen på assurans ändrats över tiden i utveckling och granskning av Försvarsmaktens IT-system?

När det gäller förtroende mellan utvecklare och granskare indikerar respondenterna att detta är en komplicerad fråga inom Försvarsmakten. Leverantören kan ses som en potentiell motståndare som vill hemlighålla sina eventuella brister för att skydda sitt rykte.

Det upplevs som att upphandlingsprocessen idag inte är anpassad för att väga in leverantörsförtroende. Åtminstone historiskt har det varit svårt att få till stånd lämpliga avtal med leverantörerna. Från leverantörernas sida upplevs det däremot som att det från Försvarsmaktens sida finns alltför stor tyngdpunkt på krav. Detta i kontrast mot att Försvarsmakten i andra sammanhang gärna talar om behov och förmåga snarare än krav och lösning.

3.6 Grundfråga 6

Hur har synen på riskavvägningar och assurans utvecklats i andra länder?

Medan säkerhetstänket alltjämt upplevs vara absolut inom svenska Försvarsmakten finns indikationer i intervjusvaren på att vissa andra länder anammat en mer relativ syn. Exempelvis har leverantörsförtroende internationellt fått ökat fokus de senaste åren. Detta illustreras bland annat av mer lagreglering av leverantörerna samt en starkare syn på regelefterlevnad. Dessutom har leverantörernas processer blivit mer intressanta. En del utländska försvarsmakter verkar ha närmat sig en acceptans av att det är näst intill omöjligt att fullständigt granska produkter genom källkodsanalys och liknande. Vidare påpekar flera respondenter att det inte räcker med förtroende för huvudleverantören utan hela kedjan av underleverantörer behöver tas i beaktande.

3.7 Grundfråga 7

Hur har byggsätt, till exempel arkitektur och komponenter, ändrats över tiden?

En vanlig typ av säkerhetsarkitektur som funnits länge baseras på lökprincipen, där systemet skyddas av flera olika lager. Det är dock möjligt att denna arkitektur överskattats och att vissa kritiska exponeringspunkter kvarstår, exempelvis vid sammankoppling med andra system eller i den underliggande hårdvaran som till och med kan ha påverkats redan vid tillverkning. Luftgap har visat sig vara otillräckligt mot särskilt resursstarka angripare som utnyttjar att användarna inte skiljs från systemet på samma sätt som tekniken. Vidare har virtualisering vuxit fram som en allt viktigare teknik och där sätts på sätt och vis luftgapet ur spel.

Perimeterskyddet innebär en tydlighet som underlättar för angriparen att hitta systemet. En tanke vore att kontinuerligt flytta systemet även om terminalerna fortsatt måste vara statiska i rummet. Relaterat till detta är huruvida systemet ska vara distribuerat eller centraliserat. Ett lokalt nät kan visserligen ge ökad tillgänglighet eftersom det inte finns en kritisk länk mellan lokalt och centralt, men samtidigt ställs då krav på lokal driftspersonal och den organisationsgemensamma helhetsbilden försvinner. Centralisering ger dock ökad kontroll över informationen och dess sekretess. Detta kan kombineras med en tunn klient som är lättare att ta med sig. Samtidigt kan detta vara ett olämpligt upplägg i en

operativ miljö eftersom en störd länk till centrala data kan ge stora konsekvenser för en pågående operation. Respondenterna indikerar dock att högsäkerhetssystem vanligen används på mindre tidskritisk, strategisk nivå.

Sammansättningar av system ger arkitektoniska utmaningar. Många tekniska lösningsförslag har presenterats som sägs underlätta och automatisera import och export av information mellan system. En kategori är dioder och slussar som ser till att bara rätt information rör sig mellan systemen och bara i rätt riktning. En annan kategori är karantäner och sandlådor som avskiljer det aktiva systemet från exponeringen utåt. Komplexa filformat är dock svåra att kontrollera ur informationssynpunkt och avseende skadlig kod, och det är oklart hur väl föreslagna lösningar passar in i den svenska försvarsmaktsmodellen. Vidare innebär import och export av information exponering och därmed kan tillförlitligheten äventyras och överbelastning inträffa.

En metod för ökad säkerhet som togs upp under intervjuerna är att använda vitlistning, som kan kompensera för oförutsedda säkerhetshål. Nackdelen är att en sådan metod kan leda till allt för säkerhetsorienterad riskavvägning till nackdel för verksamhetsnytta och tillgänglighet. Även svartlistning är en tänkbar säkerhetsmekanism, men då är risken att säkerheten blir eftersatt till förmån för verksamhetsnyttan. Trenden verkar gå mot att tillverkare anammar ett förhållningssätt som är allt mer säkerhetsmedvetet med säkra grundinställningar snarare än osäkra, även om mycket kvarstår på det området.

Ytterligare en möjlighet är att nyttja diversifiering, där någon form av redundans används för att hindra antagonistiska hot (till skillnad från den vanliga användningen av redundans där det skyddas mot icke-antagonistiska och rent driftsorienterade hot). På så vis kan de kritiska säkerhetspunkterna i systemet kompletteras av liknande men något olika skydd. Exempelvis kan snarlika komponenter från flera olika tillverkare införas eller anställda roteras mellan roller. Särskilt känsliga komponenter kan bytas ut med vissa mellanrum. Allt detta medför att en angripare måste ta sig igenom fler hinder, vilket ställer större krav på angriparens resurser. Till exempel får en angripare som lyckas infiltrera leverantörskedjan för en produkt se sitt jobb ogjort om det tilltänkta målet byts ut mot en komponent från en annan leverantör. Samtidigt ställer detta vissa krav på ökade resurser även hos försvararen.

3.8 Grundfråga 8

Hur är synen på färdiga byggstenar såsom COTS, öppen/sluten källkod och liknande?

Produkter färdiga att mer eller mindre plocka från hyllan har vuxit fram som ett alternativ till att utveckla nytt från grunden. Denna typ av produkter går ofta under benämningen off-the-shelf (OTS) med varianterna commercial off-the-

shelf (COTS) och military off-the-shelf (MOTS) beroende på tänkt kundgrupp. De senaste 15 åren har egenutveckling och erfarenhetsbaserad utveckling successivt ersatts av COTS. Existensen av färdiga komponenter gör det enklare att överallt i organisationen bygga eget. I lokala delar kan detta ge en snabbhet men också en potentiell säkerhetsrisk.

Det är svårt att hinna uppnå samma nivå av granskning själv som det går att få hos en redan existerande produkt tillverkad av ett stort välkänt företag med omfattande testprocedurer. I detta finns stora tidsvinster och möjligen vissa säkerhetsmässiga vinster att göra.

Vissa av respondenterna upplever det som tveksamt om COTS verkligen kan ha tillräcklig säkerhet. Utvecklingsmetodiken i företag är generellt sett agil snarare än baserad på den vattenfallsmodell som upplevs finnas inom den militära sfären, med egen utveckling och strävan mot absolut säkerhet. Mindre formell utvecklingsmetodik leder visserligen till snabbare uppnådd verksamhetsnytta, men det är tänkbart att företagens produkter inte når adekvat säkerhet förrän efter en viss mognadsperiod. Till exempel har Windows traditionellt nått en rimligt hög säkerhetsnivå först med större uppdateringar något år efter det att en ny operativsystemsversion har släppts. Avseende detta verkar den kommersiella marknaden ha fokuserat på bra-att-ha-funktioner snarare än på säkerhet. En annan aspekt av detta är bakåtkompatibilitet som tillåter produkter att fungera med äldre versioner. För verksamhetsnyttofunktioner är detta visserligen positivt, men säkerhetsmässigt blir angreppsytan större och begränsas av den svagaste komponenten. Ytterligare en aspekt av det agila tänket är att produkttänket ersätts av tjänster där licenser ska valideras online snarare än att en produkt körs offline. Detta är en utmaning för högsäkerhetssystemen som normalt måste vara avskilda från internet.

Även om COTS-produkter kan vara färdiga att köra i vissa standardiserade fall, måste de ofta anpassas för att passa in i den specifika systemmiljön och verksamheten. En avvägning som då måste göras är om produkten ska anpassas eller om arbetssättet eller säkerhetskraven istället kan förändras för att dra nytta av så mycket som möjligt av den befintliga produkten. En annan möjlighet är att försöka få tillverkaren att utveckla anpassade varianter av produkten. Intervjusvaren visar dock att även större militära aktörer kan ha svårt att ha tillräcklig ekonomisk styrka eftersom de inte beställer tillräckligt många enheter. Vidare gör exempelvis Natos klareringstänk – som skiljer sig från den svenska modellen – att det blir svårt för Försvarsmakten att dra nytta av de anpassningar som sker för Nato. Samtidigt gör anpassningar att många av de timmar av testning som den ursprungliga produkten genomgått inte har någon relevans för kvalitetssäkringen av den anpassade produkten. De produkter som levereras med öppen källkod är enklare att anpassa och standardiserade gränssnitt och större produktsviter ger tydligare gränssnitt mellan produkterna.

Respondenterna betraktar öppen källkod som delvis positivt. Det är enklare att själv uppdatera systemet vilket leder till mindre leverantörsberoende. Det går dessutom att inspektera koden samt skaffa sig en uppfattning om vilka beroenden som finns mellan produktens olika delar. Visserligen kommer även potentiella hotaktörer ha tillgång till koden, men kvalificerade motståndare kan i vilket fall som helst få tag i den källkod de behöver för angrepp. Dock är kod över en viss storlek i praktiken omöjlig att fullständigt kodgranska. I de fall källkoden bara är delvis öppen – som vid särskilda källkodsdelningsprogram – går det heller inte att vara säker att koden faktiskt är den som ligger till grund för den levererade produkten. Slutligen indikerar respondenterna att det finns en oro för att det blir svårt att få support för produkter som är öppna men saknar en tydlig drivande utvecklingskraft. Även om källkoden finns tillgänglig är det ofta inte önskvärt att behöva klara sig på egen hand.

4 Analys utifrån datamaterialet

I analysen som ligger till grund för detta kapitel har respondenternas utsagor sorterats i grupper baserat på samhörighet. När grupperna uppfattades som stabila namngavs de och bildade kategoriindelningen. Utsagorna i respektive kategori har därefter tolkats och sammanfattats i löpande text. Detta har gjorts baserat på ord och fraser från utsagorna för att fånga stilen och känslan i datamaterialet. Ingen ytterligare bearbetning har gjorts, utan den löpande texten för varje kategori beskriver de insamlade utsagorna på ett så källtroget sätt som möjligt.

De kategorier som identifierades i analysen av intervjusvaren var:

1. verksamhetsnytta
2. hot och risk
3. krav
4. arkitektur
5. off-the-shelf
6. leverantörsförtroende
7. insiders
8. drift.

Trots att kategorierna är baserade på intervjusvaren går det att se en koppling till grundfrågorna, vilket kan förklaras av att kategorierna speglar ett antal vanliga frågeställningar som även syns i grundfrågorna.

4.1 Verksamhetsnytta

Kategorin verksamhetsnytta inbegriper den huvudsakliga nyttan med systemet, det vill säga det verksamhetsstöd systemet ger. Två olika aspekter kunde urskiljas; den första var komplexitet, den andra var tillgänglighet och riktighet. Med komplexitet menas hur olika faktorer medverkar till ett svåröverskådligt och svårhanterligt system.

Respondenterna lyfte fram att det fortfarande finns ett stort fokus på sekretess i militära kretsar. Riktighet och tillgänglighet börjar dock få visst fokus. Riktighet har två olika men lika viktiga aspekter där den första handlar om att informationen har ett betrott ursprung och den andra om att informationen inte har ändrats sedan den kom in i systemet. En möjlighet är att begreppet riktighet utvidgas för att omhänderta båda dessa aspekter. Vidare börjar tidsaspekten komma in i bilden och den allt större komplexiteten, exempelvis på grund av bra-att-ha-funktioner, gör det allt svårare att säkra systemen och informationen.

4.2 Hot och risk

Kategorin hot och risk kan delas upp i en hotaspekt och en riskaspekt. Hot innefattar hotaktörer, potentiellt skadliga händelser samt förknippade tillfällen, motivationer och angriparresurser. Risk rör framförallt avvägningen mellan potentiell inverkan av olika intressen relaterade till systemet, såväl vänligt inställda som antagonistiska, och hur denna avvägning bör hanteras.

Respondenterna poängterade att kapplöpningen mellan angripare och försvarare fortsätter samtidigt som det är oklart hur hotinformation och kunskap ska delas för ett effektivt och samordnat försvar. Effektiva riskanalyser kräver ledarskap med helhetsbild, intressentkommunikation och en balanserad riskavvägning, snarare än överdrivet fokus på säkerhet.

Vid utveckling av IT-system för Försvarsmakten beskrivs en utpräglat konservativ inställning till tekniska lösningar. Beprövade tekniker och metoder ses som fördelaktiga eftersom deras egenskaper upplevs som väl förstådda. Nya lösningar introducerar en större grad av okända egenskaper, något som skapar osäkerhet om huruvida förståelsen för säkerhetsegenskaperna är tillräckliga för att resultatet ska gå att lita på. För högsäkerhetssystem är detta förstås problematiskt och därmed oönskat. Valet faller därför i allmänhet på återanvändning hellre än nyutveckling, även i de fall nya lösningar erbjuder större verksamhetsnytta.

4.3 Krav

Kategorin krav innefattar en mer specifik tolkning av behov. Dessutom inkluderas olika aspekter relaterade till granskningsförfarandet, som ska säkerställa att kraven uppfylls, samt olika former av säkerhetstester.

Respondenterna tar upp att det finns ett fokus på krav snarare än på behov och förmågor. Detta leder till omfattande granskningsprocesser som fördröjer utvecklingen i åratal. Samtidigt finns ingen uppföljning över tiden. KSF3 har inte fått önskat genomslag och en tydligare separation mellan kravställare och granskare behövs, liksom en acceptans för att det inte går att kontrollera allt.

4.4 Arkitektur

Kategorin arkitektur omfattar de övergripande ramarna för systemlösningarna. Arkitektur kan ses ur två olika perspektiv. Först och främst ett informationsfokus, där olika system och typer av information samsas och utbyts. Det andra perspektivet på arkitektur är ett systemfokus där själva ramarna syns tydligt.

Många respondenter pekar på att det är essentiellt att koppla samman informationsobjekt och system. Ansvarsfördelningen mellan de sammankopplade systemen är dock oklar och frågan är hur mogen tekniken är. Det är en utmaning

att klassificera stora informationsmängder. Vidare gäller det att inte lägga alla ägg i samma korg och använda en och samma säkerhetsfunktion/mekanism eller en viss leverantör i för hög utsträckning. En arkitektur behöver väga behovet av att kunna agera autonomt mot kontrollen av data och den organisatoriska helhetsbilden som centralisering kan ge. Tunna klienter och lokala autonoma nät kan i vissa fall vara en bra balansgång.

4.5 COTS

Inom kategorin COTS återfinns aspekter som rör påverkan av huruvida systemet byggs med befintliga komponenter respektive egenutvecklade komponenter.

Respondenterna anser att COTS är mer agilt, tjänstebaserat och vältestat. Samtidigt erhålls eventuellt inte lika hög säkerhet och det är svårt att ställa krav, även för aktörer som i andra sammanhang är mycket stora. Detta leder till utmaningar kring anpassning, bland annat kan arbetssätt behöva ändras för att få maximal nytta av redan existerande produkter.

Kategorin COTS är väsentligen densamma som grundfråga 8 som redovisas i avsnitt 3.8, varför en längre beskrivning undviks här.

4.6 Leverantörsförtroende

Kategorin leverantörsförtroende berör hur det går att skapa tilltro till en leverantör och dess produkter eller tjänster, snarare än att direkt kontrollera och testa det som levereras. I kategorin ingår även förhållandet till underleverantörer.

Respondenterna tar upp leverantörsförtroende som ett område som fått mer fokus internationellt. Snarare än att försöka säkra produkterna in absurdum ägnas det nu mer kraft åt att kontrollera och säkra processerna. Det är viktigt att säkra hela leverantörskedjan, att skaffa tilltro till andra parter och att kunna sluta passande avtal.

4.7 Insiders

Kategorin insiders omfattar hanterandet av både välvilliga användare på olika nivåer – däribland slutanvändare, administratörer och driftspersonal – samt hur antagonister på insidan kan hindras från att skada systemet och dess relaterade nyttofunktion.

Respondenterna pekar på att insiderhotet är det som kvarstår när de tekniska bitarna säkrats. Det har den senaste tiden blivit mer accepterat att tekniken faktiskt inte kan lösa allt. Personlig autentisering och spårbarhet är försök att

adressera insiderproblematiken tillsammans med mjukare lösningar som rolluppdelning och flerhandsfattning.

4.8 Drift

Kategorin drift rör det aktiva systemskedet då systemet används. Skedet berör aspekter som att säkerheten övervakas och upprätthålls vid drift och avvägningen mellan att ändra systemet i avsikt att göra det bättre men att då riskera att istället göra det sämre.

Respondenterna anser att det behövs en kontinuerlig och snabbreagerande drift av systemen snarare än en tro på att allt går att lösa under systemutvecklingen. Detta förutsätter dock resurser och att systemet designats med drift och driftsmiljön i åtanke.

5 Resultat

Kapitel 3 och 4 beskriver bredden av de åsikter som återfinns hos respondenterna, men visar inte hur vanligt förekommande åsikterna är eller vilken tyngd respondenterna lagt vid dem. För att lyfta fram huvudfårorna i åsikterna beskriver detta kapitel några särskilda teman. Till skillnad från analyskapitlen omfattar temana inte hela det studerade området. Istället är dessa teman sådana för vilka samstämmigheten var särskilt påtaglig och uppfattas därför ha en tillräckligt hög grad av representativitet för att fungera som svar på huvudfrågan.

I respondenternas svar kan ytterligare intressant information skönjas som ligger utanför studiens huvudfråga. Denna information är mer i form av nya frågeställningar som inte var möjliga att besvara inom ramarna för den aktuella studien. Dessa frågor formuleras i appendix B och är huvudsakligen av bredare karaktär, exempelvis avvägningar och förhållningssätt inom olika områden nära studiens frågeställningar.

5.1 Absolut säkerhet är omöjlig

Intervjuerna genomsyras av uppfattningen att absolut säkerhet, med starkt fokus på sekretess, driver IT-säkerhetsarbetet medan tillgänglighet och verksamhetsnytta får stå tillbaka. Kryptering används flitigt även om det kan ställa till problem vad gäller backuper och leda till arbetsamma rutiner för användarna. Vitlistning kompenserar för oförutsedda hål men kan leda till alltför stort fokus på sekretess, till nackdel för verksamhetsnytta och tillgänglighet. Samtidigt pekar flera respondenter på att många säkerhetsmekanismer som möter sekretessbehovet även ger ökad tillgänglighet. Vidare finns en skillnad mellan Försvarsmaktens absoluta säkerhetstänk och den inställning som är förhärskande på den civila sidan. Civila företag är betydligt mer förknippade med agila systemutvecklingsprocesser vilket ger lättrörligare och mer anpassningsbara produkter.

Absolut säkerhet har tidigare varit ett rimligt mål, men har blivit allt svårare att uppnå under de senaste 15 åren. En betydande orsak är att IT-systemen blivit mer omfattande och komplexa. Tekniken har förbättrats i hög takt vilket gett billigare lagringsmedia och större beräkningskraft. I samband med detta har anslutningarna ökat och därmed också både datamängderna och antalet användare. Dessutom har den generella funktionsrikedomen gjort att systemen innehåller mer än bara det som faktiskt behövs. Komplexiteten ökar antalet systemdelar och gör det svårare att veta vad systemet består av. En annan del där detta märks är mängden källkod som nått långt över den gräns där allt kan granskas. En anledning är att programmering av systemen sker på allt högre nivå för att kostnadseffektivisera och underlätta utvecklingsarbetet, men till kostnaden av allt större kodmängder i systemen då varje nivå introducerar ett nytt lager av översättning ned mot maskinkod och nya bibliotek med funktioner som inkluderas i systemet. Vidare

har det insetts att hårdvara är mycket komplicerad och det finns en hotbild som rör manipulation av även de allra minsta av komponenter. Tillsammans gör dessa faktorer att absolut säkerhet blir allt svårare att ha som mål.

För att minska fokus på absolut säkerhet måste systemägarna kunna göra en aktiv avvägning mellan olika säkerhetsaspekter. Ett område där en riskavvägning måste göras är patchning. En patch som lagar ett säkerhetshål kan inte alltid testas till fullo innan den införs, eftersom testtiden kan leda till att en angripare hinner utnyttja säkerhetshålet. Införandet av bristfälligt testade patchar kan dock i sig medföra nya säkerhetsbrister.

5.2 Kommunikationen mellan IT-system har ökat

IT-system utbyter allt mer information. För att säkerställa att information inte flyttas åt fel håll mellan två system eller att fel information utbyts och sekretessen äventyras, finns en rad olika föreslagna lösningar såsom slussar, dioder, sandlådor och karantäner. Komplexa filformat är dock svåra att kontrollera både ur informationssynpunkt och avseende eventuell skadlig kod, medan arvssystem leder till skillnader i protokoll. Detta gör snabba och automatiska kontrollmekanismer svåruppnåeliga. Dessutom måste import- och exportfunktioner säkerställa att systemen inte överbelastas och att information inte läcker mellan systemen. Att nyttja traditionella perimeterskydd vid sammankopplingar är besvärligt. Ett alternativ som nämnts är ett mer informationsbaserat skydd där systembegreppet löses upp och ersätts av skydd för enskilda informationsobjekt eller mindre mängder av informationsobjekt.

5.3 Ackrediteringsprocessen är hindrande

Att försöka uppnå absolut säkerhet ger kravfokus och därigenom granskningsfokus. På så vis läggs stor möda på att kontrollera produkter och lösningar på ett omfattande sätt. Detta innebär en hög kostnad och granskningsprocessen kan leda till flera års fördröjningar. Dessutom blir det svårt att avgöra om system överhuvudtaget kommer att godkännas och i så fall när. Ovissheten i tid kan dessutom leda till att en föreslagen lösning som får avslag av granskaren inte omarbetas utan att granskaren istället föreslås en aningen justerad variant och ett säkerhetens lapptäcke tar plats.

Med tanke på att IT-systemen växt i storlek de senaste 15 åren blir det allt svårare att med manuella rutiner åstadkomma en tillräckligt snabb granskning. Vidare tyder intervjusvaren på att det finns en uppfattning i Försvarsmakten om att all granskning måste göras inom organisationen snarare än att åtminstone delvis kunna förlita sig på de tester som utvecklarna redan utfört. Därmed

utnyttjas inte värdet av en stor mängd testtimmar samtidigt som det är svårt att uppnå samma nivå av kvalitetssäkring på egen hand. Dessutom verkar ackrediteringen i mångt och mycket vara ett engångssteg snarare än en kontinuerlig livscykelprocess. Vartefter system förändras skiljer därmed allt mer mellan systemet som granskades och systemet som är i drift.

KSF3 föreskriver att systemets kontext ska vägas in i kravställning och granskning. Därmed behöver ett mindre exponerat system inte uppfylla lika hårda säkerhetskrav som ett mer exponerat system. Vidare var det tänkt att realiseringsförslag för olika säkerhetslösningar skulle införas i KSF3. Dessa ansatser kunde dock inte genomföras fullt ut och gav inte önskat genomslag. Därmed är det fortsatt svårt att på säkerhetsområdet väga in nytta och kostnad samt anamma en mer reaktiv riskhantering. Ett alternativ till produktfokus är att sätta sin tillit till leverantörernas utvecklingsprocesser för att på så vis avgöra om en produkt är säker. Både leverantörernas egna processer samt underleverantörernas processer är då av intresse. Idag finns dock begränsningar kring detta. Exempelvis är det svårt att använda leverantörsförtroende som kriterium i avtals- och upphandlingsprocesser. Dessutom kan leverantören vilja hemlighålla eventuella brister för att undvika att förlora sitt goda rykte och därmed förlora köparnas förtroende.

5.4 IT-säkerhet kräver kontinuerligt säkerhetsarbete

Om fokus på absolut säkerhet ska minska, och därmed även det relaterade säkerhetsarbetet tidigt i systemets livscykel, behövs ett kontinuerligt och aktivt säkerhetsarbete under driftsfasen. Respondenterna lyfter fram övervakning, logganalys och penetrationstester som viktiga. Vidare behövs omvärldsbevakning när det gäller såväl hot som komponenter. Det kan då vara lämpligt att samarbeta med andra för att få så mycket hot- och sårbarhetsinformation som möjligt, samtidigt som det kan vara svårt att dela information om specifik hotbild eftersom den kan vara hemlig. När sårbarheter upptäckts är det dessutom inte rättframt att applicera lämpliga patchar. Säkerhetshålet kan behöva täppas till skyndsamt samtidigt som patchen kan ta tid att testa ordentligt, särskilt om en ny ackreditering krävs. Används en anpassad version av COTS måste patchen kanske dessutom anpassas innan den kan appliceras. Testmiljöer kan dock till viss del underlätta tester av patchar.

För ett effektivt säkerhetsarbete kan driftspersonalen behöva samordnas fysiskt. Detta begränsar dock möjligheten till support på mer lokal nivå. Generellt är det viktigt att redan vid systemets initiala utveckling tänka på att skapa en driftvänlig miljö.

6 Diskussion

Resultatkapitlet är i hög grad problemfokuserat och det beskrivs många tankar bland personer inom området om hur saker kan göras annorlunda. Det är dock värt att notera att parallellt med dessa uppfattningar om utmaningar och önskad förändring fanns en tydlig förståelse för behovet av effektivt skydd och en stor acceptans för att skydd kan ge effekter på systemens funktion och användbarhet. Studien visar inte på något missnöje med Försvarsmaktens höga ambitioner på informationssäkerhetsområdet, utan tvärt om beskrivs genomgående en vilja att såväl följa gällande regler som att agera insiktsfullt och eftertänksamt.

I dagens svenska regelverk går det att se hur riskavvägningar har börjat komma in i IT-säkerhetsarbetet, till exempel i form av de exponerings- och konsekvensnivåer som infördes i KSF3 samt att riktighet och tillgänglighet har fått större fokus i säkerhetsanalyserna. Detta är dock endast ett litet steg på vägen till riskbaserad säkerhet i IT-system och det skulle krävas omfattande ändringar i hur system utvecklas, ackrediteras och förvaltas för att nå hela vägen. Målbilden borde i så fall vara att ta fram metoder för att utveckla och förvalta system som löser verksamhetens behov tillräckligt bra med en känd och acceptabelt låg risknivå för att ge värde till verksamheten samtidigt som kostnaderna kan hanteras. I detta ingår att kontinuerligt vidmakthålla systemet på ett sådant sätt att risken hela tiden beaktas och att den inte stiger till en oacceptabel nivå.

Författarnas erfarenhet är att utvecklingen i IT-branschen under de senaste 10–15 åren inneburit att användarnas förväntningar på systemen har förändrats och att acceptansen för svårhanterade IT-system har minskat. De möjligheter som ges med modernare IT-stöd har blivit tydligare för användarna, vilket innebär att avsaknad av detta kan upplevas som ett hinder i arbetet och leda till frustration.

Det finns även en fara för mer direkt påverkan på verksamheten då system som skulle underlätta eller rentav möjliggöra verksamhet inte byggs och driftsätts. Anledningen till att systemen inte byggs kan vara såväl resursbrist, exempelvis för att bekosta utvecklings- och ackrediteringsarbetet som krävs för att nå dagens säkerhetskrav, som att nya arkitekturer och byggsätt inte accepteras då de kan medföra att en ökad säkerhetsrisk i något avseende måste accepteras i systemet.

Ett annat förhållningssätt till IT-säkerhetsrisker skulle ge möjlighet att använda nya arkitekturer och funktioner i IT-systemen, vilket har potential att ge större verksamhetsnytta och kostnadseffektivitet. En möjlighet skulle vara att i större omfattning använda kommersiella systemkomponenter, vilka skulle ge ekonomiska fördelar som storskalighet i utveckling och produktion samtidigt som de i många fall är genomtänkta ur både administrations- och användarperspektiv. Ett nytt förhållningssätt skulle medföra potentiellt ökade IT-säkerhetsrisker som då måste balanseras mot den nytta som systemet skapar, och i de fall där nyttan överstiger IT-säkerhetsrisken skulle riskerna kunna vara acceptabla.

En förändring av de grundläggande principerna i ackrediteringsarbetet är en omfattande och komplex process där många intressenter är inblandade. Sannolikt skulle förändringar krävas på ett flertal nivåer, exempelvis i de övergripande interna bestämmelserna om IT-säkerhet i Försvarsmakten, i hur ansvar fördelas runt kravställning och ackreditering samt i hur detaljkrav utformas inom IT-säkerhetsområdet. En av de åsikter som togs upp av respondenterna och som relaterar till ansvarsfördelningen är problematiken med att samma instans i stor utsträckning både kravställer och godkänner säkerhetslösningarna i systemen samt att denna instans inte har en direkt koppling till verksamheten. Detta innebär att verksamhets- och säkerhetskraven kommer från olika källor med följden att kraven ofta står i konflikt med varandra. I ackrediteringsprocessen är det lätt att säkerhetskraven får större tyngd än den verksamhetsnytta som systemet är tänkt att skapa då verksamhetens behov inte vägs in tillräckligt i riskanalysen.

Enligt Försvarsmaktens interna bestämmelser (Försvarsmakten 2006) har Militära underrättelse- och säkerhetstjänsten (MUST) ett explicit utpekat ansvar vid ackreditering av IT-system och godkännande av vissa IT-säkerhetskomponenter. Detta innebär att MUST har ett stort ansvar inom IT-säkerhetsområdet och ett tydligt mandat i vissa frågor inom området. För andra frågor är ansvarsfördelningen inte lika tydlig varför det finns en osäkerhet om MUST:s mandat, vilket författarna har uppfattat ger en utbredd känsla av att MUST i praktiken får vetorätt i nästan alla IT-säkerhetsfrågor då det sällan är någon som är beredd att ta det ansvar som det innebär att avvika från rekommendationerna i MUST:s yttranden. MUST har en naturligt försiktig hållning när det gäller IT-säkerhetsrisker, vilket är helt rimligt då det är deras ansvar att peka på risker och potentiella säkerhetsbrister i systemen. Problemet uppstår då ett restriktivt yttrande tolkas som ett absolut avslag på en lösning, trots att ingen övergripande riskanalys har gjorts för att se om risken som påpekas i yttrandet är oacceptabel, om den är hanterlig på systemnivå eller om den kan accepteras då verksamhetsnyttan väger tyngre.

Det är viktigt att poängtera att författarna inte ser de identifierade problemen som MUST:s ansvar eller ”fel” eftersom situationen har uppstått genom otydligheter i hur ansvaret för IT-säkerhet fördelas inom Försvarsmakten. Författarna anser att MUST:s roll som sammanhållande aktör i IT-säkerhetsarbetet är värdefull och nödvändig även om ansvarsfördelningen förändras eller förtydligas.

Slutsatsen är att dagens situation inte är tillfredsställande och att detta delvis kan ha uppkommit på grund av oklar ansvarsfördelning inklusive oklarheter i hur avvägningar mellan verksamhetens behov och IT-säkerhet ska göras. Sammanvägt med övriga frågor som tagits upp i diskussionen ovan ges en bild av att det bör genomföras en genomgripande utredning av hur IT-säkerhetsaspekter ska hanteras när Försvarsmakten tar fram och förvaltar IT-system för att bättre kunna tillgodose verksamhetens behov i framtiden.

Källförteckning

Försvarsmakten (2006). *Försvarsmaktens interna bestämmelser om IT-säkerhet*. FIB 2006:2.

Försvarsmakten (2012). *Krav på IT-säkerhetsförmågor hos IT-system v3.0*.

Kvale, S. (1997). *Den kvalitativa forskningsintervjun*. Lund: Studentlitteratur.

Strauss, A. och Corbin, J. (1998). Basics of qualitative research, Thousand Oaks, California, USA: SAGE Publications.

Appendix A. Intervjufrågorna

Frågorna till intervjuerna listas nedan.

- Berätta lite om...
    - …din FM-bakgrund eller motsvarande i annan organisation, utbildning, tidigare projektverksamhet, ...
    - …din erfarenhet av högsäkerhetssystem/sekretesskydd?
    - …du har någon anknytning till en leverantör inom IT-området?
- Hur upplever du att större, IT-baserade informationssystem har utvecklats under de senaste 15 åren?
    - Vilken betydelse har utvecklingen haft för funktionaliteten i systemen?
    - Vad har utvecklingen haft för betydelse för säkerheten i systemen?
- Används andra IT-arkitekturer för system med höga krav på sekretess, motsvarande H/S-H/TS, än för system utan dessa krav?
    - Är arkitekturlösningarna för sekretess annorlunda än för andra säkerhetsaspekter såsom integritet och tillgänglighet?
- Har utvecklingen av IT-arkitekturen för system med höga krav på säkerhet sett annorlunda ut än för ”normala” IT-system?
    - Har utvecklingen av ”normala” system haft inflytande på högsäkerhetssystemens utformning och i så fall hur?
    - Om inget/litet inflytande: Vad har hindrat utvecklingen från att influera högsäkerhetssystemen?
- Bygger man säkerhet med arkitektur eller specifika säkerhetslösningar/-funktioner?
    - Hur förhåller sig arkitekturlösningar till specifika säkerhetslösningar/-funktioner när det gäller hög säkerhet?
    - Vilka arkitekturkonstruktioner är basen i dagens högsäkerhetssystem?
    - Hur ser du på specialutvecklade komponenter kontra COTS för säkerhetslösningar?
    - Hur ser du på open source kontra closed source för säkerhetslösningar/-funktioner?

- Har den tekniska hotbilden mot högsäkerhetsystemen förändrats under de senaste 15 åren?
    - Hur har förändringen av hotbilden påverkat utvecklingen av funktionalitet i systemen?
- Vilka aspekter bör man ta hänsyn till när man värderar exponeringen för ett högsäkerhetssystem?
    - Hur stor exponering är rimlig?
    - Hur många användare är rimligt?
    - Hur bör man hantera systemadministratörer? Spårbarhet för deras arbetsuppgifter?
    - Hur tillgängliga är det rimligt att terminalerna är?
    - Hur ser du på en distribuerad kontra centraliserad arkitektur?
- Hur kan man hantera försörjningen av extern data/grunddata till högsäkerhetssystem?
    - Hur kan man hantera information med olika klassificering separerat i ett system?
    - Hur kan man märka informationen med klassning på ett säkert sätt?
    - Vad krävs av anslutande system som försörjer systemet med information?
    - Hur kan man hantera uppdateringar och patchar av systemet på ett säkert sätt?
- Upplever du att förväntningar på granskning och ackreditering påverkar systemlösningen?
- Har du sett exempel på där hanteringsreglerna runt sekretess har ändrats för att passa modernare arbetssätt och därmed modernare arkitektur?
    - Har du några tankar om klassificering med tidsgräns?
- Har säkerhetsmålsättningarna (säkerhetskraven) förändrats över de senaste 15 åren?
    - Hur mycket påverkar säkerhetsmålsättningen/-kraven systemens uppbyggnad idag? På vilka sätt?
    - Vilken inverkan har dagens assuranskrav? (På systemet och utvecklingsarbetet.)

    - Hur sker kontinuerlig uppföljning av säkerheten under användningsfasen?

- Hur ser du att utvecklingen kommer att vara för storskaliga högsäkerhetssystem?
    - Är frågeställningarna som tagits upp under intervjun något som diskuteras?
    - Vad tror du är värdefullt för att föra utvecklingen vidare?
    - Tror du att arbetssätten i högsäkerhetssystem kommer ändras som resultat av IT-systemens nya möjligheter?
- Har du något att tillägga eller några frågor? Är något mer som vi borde känna till eller tänka på angående det vi pratat om?

Appendix B. Frågor som identifierats i analysen

Under analysarbetet identifierades ett antal ämnen som uppfattades som viktiga men som inte låg inom ramen för studien. Dessa ämnen får betraktas som ett resultat av såväl respondenterna som författarna. Då dessa ämnen ansågs relevanta återges de i detta appendix i form av frågor sorterade efter samma kategorier som använts i kapitel 4. En tänkbar användning för dessa frågor är som utgångspunkt för framtida forskning.

1. Verksamhetsnytta

1.1. Hur kan tilltro till information samt hot utan hotaktörer hanteras för att ge en helhetssyn på säkerhet?

1.2. Hur tas mer hänsyn till tidsaspekten för att maximera nyttan kontra risk och därmed bara ställa krav på säkerhet så länge den behövs?

2. Hot och risk

2.1. Hur kan hotinformation och trender delas utan att känslig information sprids?

2.2. Hur förenklas riskanalyser och vem ska ta ansvaret för att gå från riskaversion till en mer balanserad riskavvägning?

3. Krav

3.1. Hur kan kraven omstruktureras för att hålla över tiden, sätta fokus på förmågor och tillåta att COTS på allvar kan övervägas?

4. Arkitektur

4.1. Hur mogna är de tekniker som låter system utbyta information på ett kontrollerat sätt?

4.2. Skulle det vara fruktbart med ett annat synsätt där informationsobjekt snarare än system skyddas? Går det rentav att låta objekten skydda sig själva?

4.3. Vilka systempunkter är mest sårbara och var kan diversifiering hjälpa?

4.4. Vilken avvägning av centralisering/distribuering är lämplig för vilken typ av verksamhet? Kan man skapa en vägledande indelning?

5. COTS

5.1. Vilken avvägning är lämplig mellan anpassning av COTS och anpassning av rutinerna?

6. Leverantörsförtroende

6.1. Hur erhålls tillräckligt förtroende för leverantörer och underleverantörer samt går det att väga in detta vid upphandling?

7. Insiders

7.1. Vad avgör om personlig autentisering är stark nog och hur hanteras rolluppdelning effektivt?

8. Drift

8.1. Hur säkerställs att driftsmiljön beaktas redan under de initiala systemutvecklingsstadierna för att tillåta kontinuerlig och snabbreagerande drift?

FOI är en huvudsakligen uppdrags nansierad 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