Informationssäkerhets-egenskaper

Avvägningar och prioriteringar

AMUND GUDMUNDSON HUNSTAD

FOI-R--4341--SE
ISSN 1650-1942 December 2006

Amund Gudmundson Hunstad

Informationssäkerhets-egenskaper

Avvägningar och prioriteringar

Titel	Informationssäkerhetsegenskaper – Avvägningar och prioriteringar
Title	Information security characteristics - Considerations and priorities
Rapportnr/Report no	FOI-R--4341--SE
Månad/Month	December
Utgivningsår/Year	2016
Antal sidor/Pages	28
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E72627
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Informationssäkerhetsegenskapen *sekretess* har en framträdande roll inom Försvarsmakten, medan egenskaperna *riktighet* och *tillgänglighet* inte har getts motsvarande utrymme. Behov av att beakta riktighet och tillgänglighet lyfts återkommande, men sekretessens framträdande roll kvarstår.

Denna rapport identifierar övergripande och bakomliggande prioriteringar för att beskriva hur andra informationssäkerhetsegenskaper än sekretess ges utrymme och hanteras inom Försvarsmakten. Syftet är att därigenom påvisa möjliga avvägningar för att nå bästa möjliga balans mellan informationssäkerhets-egenskaperna.

I rapporten presenteras begreppsutvecklingen inom informationssäkerhets-området. Därefter presenteras två tänkta fall för att illustrera att sekretess, riktighet och tillgänglighet till betydande grad betraktas som oberoende aspekter med separata hanteringssätt, vilket presumtivt är kritiskt och allvarligt. En behovsbild avseende olika perspektiv på informationssäkerhetsegenskaperna inom Försvarsmakten redovisas, likaså hur de olika egenskaperna ger avtryck i centrala styrande dokument.

Studien drar som slutsats att sammanvägning av olika behovsbilder inom Försvarsmaktens verksamhetsplanering respektive operativa verksamhet har potential att ge bättre balans mellan sekretess, riktighet och tillgänglighet. Riktighets- och tillgänglighetsaspekterna bör ge tydligare avtryck i för Försvarsmakten centrala styrande dokument. Säkerhets- och riskanalyser, som åskådliggör nytta med olika informationssystem och -tjänster och identifierar risker, möjliggör eftersträvade avvägningar för att nå bästa möjliga balans mellan informationssäkerhetsegenskaperna.

Nyckelord:

Informationssäkerhet, informationssäkerhetsegenskaper, konfidentialitet, sekretess, riktighet, tillgänglighet, säkerhetsfunktioner, säkerhetsskyddslag

Summary

The information security characteristic confidentiality has a prominent position within the Swedish Armed Forces, while integrity and availability do not have a similar position. The need of taking into consideration integrity and availability is frequently stated, but the prominent position of confidentiality remains.

This report identifies comprehensive and underlying priorities to enable describing the way in which other information security characteristics than confidentiality are handled within the Swedish Armed Forces. Thereby possible considerations to obtain the best possible balance between the information security characteristics may be indicated.

The evolution of terminology within the information security domain is presented. Two potential cases are described and illustrate how confidentiality, integrity and availability to a significant degree are considered as independent aspects with separate ways of being handled, which supposedly constitutes a critical and serious problem. Comprehensive needs regarding different perspectives related to information security characteristics within the Swedish Armed Forces are presented, as well as how the different characteristics influence important policy documents.

The study concludes that aggregating different comprehensive needs related to management as well as operative level within the Swedish Armed Forces, have the potential of achieving a better balance between confidentiality, integrity and availability. Aspects of integrity and availability ought to distinctly influence policy documents of the Swedish Armed Forces. Studies of security and risk analysis, which illustrate the benefits of different information systems and services and identifies associated risks, facilitates achieving the needed considerations to reach a best possible balance between the information security characteristics.

Keywords: Information security, information security characteristics, confidentiality, integrity, availability, security functions

Innehåll

1 Inledning

Inom Försvarsmakten är *sekretess* den prioriterade informationssäkerhets-aspekten. I de flesta indelningar av vad som definierar informationssäkerhet är även *tillgänglighet* och *riktighet* två centrala informationssäkerhetsegenskaper. Den tydliga prioriteringen av sekretess hos Försvarsmakten är till betydande grad ett resultat av lagkrav som har haft en tyngdpunkt på sekretess. Avvägningar avseende restriktioner på vem som bör ges åtkomst till information är styrande, exempelvis för att avgränsa vad främmande makt ges möjlighet att ha kännedom om. Prioriteringen av sekretess kan även tänkas vara ett resultat av organisatorisk tradition, där reflektioner i termer av tillgänglighet och riktighet inte har fått motsvarande utrymme. Sekretess är en fråga av vikt för hela Försvarsmakten, medan riktighet och tillgänglighet har setts som en fråga för systemägare.

Hög sekretess kan ensamt inte säkra en tillräcklig nivå av informationssäkerhet. För de som behöver ha tillgång till information är det dessutom av vikt att denna inte har manipulerats. Därmed är även tillgänglighet och riktighet viktiga egenskaper. Det gäller att hitta balansen mellan informationssäkerhets-egenskaperna. Med detta som utgångspunkt redovisar denna rapport en inledande studie av hur andra informationssäkerhetsegenskaper än sekretess ges utrymme och hanteras inom Försvarsmakten. Målet med rapporten är att påvisa möjliga avvägningar för att nå bästa möjliga balans mellan informationssäkerhets-egenskaperna.

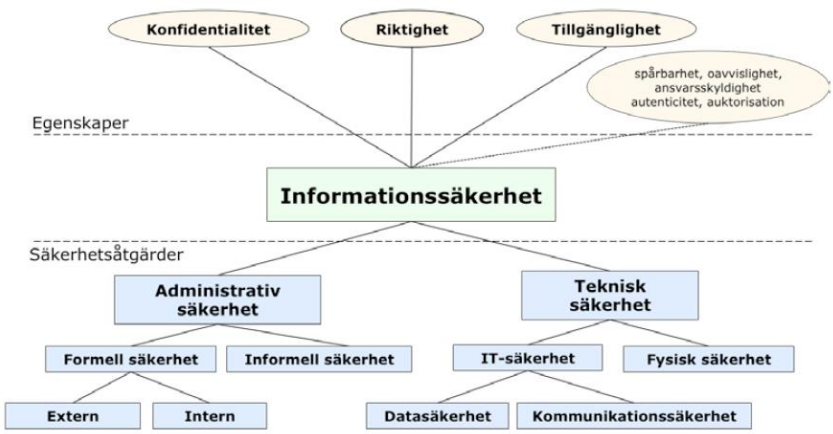
Kapitel 2 redovisar definitioner av centrala begrepp inom informationssäkerhet och hur begreppsutvecklingen i grova drag har varit sedan 60-talet. I kapitel 3 presenteras två korta tänkta fall som avses illustrera hur behoven av riktighet och tillgänglighet är tydliga och även samverkar med behoven av sekretess. Vidare presenterar kapitlet en grundproblematik i form av att de tre informations-säkerhetsegenskaperna ses som separata problemdomäner med separata hanteringssätt, vilket presumtivt är kritisk och allvarligt. Kapitel 4 redovisar ett urval av observationer och en behovsbild från en tidigare FOI-studie avseende olika perspektiv inom Försvarsmakten på centrala informationssäkerhets-egenskaper. Kapitel 5 redovisar ett urval av för Försvarsmakten centrala styrande dokument och informationssäkerhetsegenskapernas avtryck i dessa. Sammanfattande observationer och diskussion utgör kapitel 6.

2 Utmaningar och grundbegrepp inom informationssäkerhet

I detta kapitel redovisas definitioner av centrala informationssäkerhetsbegrepp, satt i sammanhang av begreppsutvecklingen inom området från sent 1960-tal och framåt.

2.1 Definitioner

Terminologi för informationssäkerhet (SIS, 2015) beskriver informationssäkerhet som bestående av såväl administrativ säkerhet som teknisk säkerhet. Informationssäkerhet inkluderar därmed även problematik avseende pappersbunden information. Fokus tenderar dock att vara på IT-baserad informationshantering.



Figur 1 Informationssäkerhetsmodell (SIS, 2015)

Figur 1 illustrerar hur informationssäkerhet relaterar till dess egenskaper samt säkerhetsåtgärder som behövs beaktas för att uppnå informationssäkerhet. I Figur 1 listade egenskaper relaterade till informationssäkerhet definieras enligt följande (SIS, 2015):

- *Konfidentialitet:* Skydd mot obehörig insyn. Sekretess används ofta i legala sammanhang och ges där en delvis annan innebörd än konfidentialitet.
- *Riktighet:* Skydd mot oönskad förändring.

- *Tillgänglighet:* Åtkomst för behörig person vid rätt tillfälle.[1]
- *Spårbarhet:* Entydig härledning av utförda aktiviteter till en identifierad användare.
- *Oavvislighet:* Tillhandahållande av teknisk bevisning för förekomsten av en påstådd händelse eller handling och dess ursprung.
- *Ansvarsskyldighet:* Principen att stå till svars och ta ansvar för konsekvenserna av beslut och aktiviteter inför organisationens styrande organ, rättsliga myndigheter och inför intressenter i allmänhet.
- *Autenticitet:* Äkthet avseende uppgivna uppgifter; särskilt rörande påstådd identitet och meddelandens ursprung och innehåll
- *Auktorisation:* Fastställande av åtkomsträttigheter för en användare.

Denna rapport utgår huvudsakligen från de tre i Figur 1 särskilt accentuerade egenskaperna *konfidentialitet*, *riktighet* och *tillgänglighet*. Dock, redan på detta tidiga stadium av rapportens diskurs manifesterar sig ett vägval kring en viktig detalj – och som bekant finns djävulen i detaljerna. I rapporten kommer resonemang kring konfidentialitet domineras av användande av termen sekretess. Visserligen är enligt (SIS, 2015) sekretess en *avrådd term*, men som definitionen klargör används begreppet sekretess ofta i legala sammanhang. I Handbok Försvarsmaktens säkerhetstjänst, Informationssäkerhet H Säk Infosäk (Försvarsmakten, 2013) används termen konfidentialitet vid tre tillfällen. Termen sekretess används däremot vid 894 tillfällen. Konfidentialitet bedöms användas i (Försvarsmakten, 2013) som ett övergripande begrepp, i vilket sekretess ingår och verkar inneha viss vikt. Vi väljer därför att i resten av rapporten fokusera på begreppen *sekretess*, *riktighet* och *tillgänglighet*.

2.2 Begreppsutveckling inom informationssäkerhet

Computer Security (Gollmann, 2011) är en bra lärobok inom informations- och IT-säkerhetsområdet, även avseende begreppsutvecklingen inom domänen. Gollman lyfter särskilt fram två rapporter som viktiga för etablerandet av IT-säkerhet som en egen vetenskaplig disciplin under 70-talet, (Ware, 1970) och (Anderson, 1972).

[1] (SIS, 2007) definierade tillgänglighet som att ”*informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid*”, vilket inte begränsar tillgänglighet till att avse personers åtkomst till informationstillgångar, vilket nu aktuell version gör.

Ware (1970) redovisar den tekniska bakgrunden för och utvecklingen inom IT-säkerhetsområdet fram till slutet av 1960-talet. Särskilt fokuserar rapporten på policykrav avseende sekretessklassificerad information inom den amerikanska försvarsmakten. Tillkomsten av fleranvändarsystem som även är geografiskt spridda utgjorde en för Ware (1970) viktig utmaning. Begreppsbildningen motsvarar inte fullt ut den gängse terminologi som idag används inom IT- och informationssäkerhetsområdena[2]. Inledningsvis talar Ware (1970) i termer av behovet av *”some sort of "privacy" protection to users who wish to preserve the integrity of their data and their programs”*. Detta indikerar en forskningsdisciplin som vid den tidpunkten hade påbörjat utvecklingen av en egen begreppsapparat, men där begreppen ännu inte hade mognat och stabiliserats.

Ware (1970) listar som förväntade egenskaper hos system följande engelska termer: flexible, responsive, auditable, reliable, manageable, adaptable, dependable och configuration integrity. Dagens närmast självklara och domändefinierande termer sekretess[3] (confidentiality), riktighet (integrity) och tillgänglighet (availability) är inte med i systemegenskapslistan. En sökning i (Ware, 1970) efter dessa tre begrepp ger följande enkla statistik:

Informations-säkerhetsaspekt	Antal träffar i (Ware, 1970)	Kommentar
Confidentiality	0	
Integrity	15	Begreppet används mer i betydelsen okränkbarhet för olika systemresurser än avseende att information inte har manipulerats eller ändrats
Availability	0	

Däremot ger sökning på *classified* 129 träffar. Användningen av begreppet *classified* i (Ware, 1970) ligger närmare hur begreppet *confidential* används idag.

Även Anderson (1972) fokuserar på krav avseende sekretessklassificerad information inom amerikanska försvarsmakten. En motsvarande begrepps-sökning i (Anderson, 1972) ger följande statistik:

[2] Även begreppen IT- och informationssäkerhet i sig har tillkommit betydligt senare.

[3] (SIS, 2015) använder dock som redan nämnts konfidentialitet, där (SIS, 2007) även använde termen sekretess, vilken fortfarande är en använd term i åtminstone legala sammanhang och i Försvarsmaktssammanhang.

Informations-säkerhetsaspekt	Antal träffar i (Anderson, 1972)	Kommentar
Confidentiality	0	
Integrity	20	*Security integrity* är ett begrepp som används, likaså används begreppet *data integrity*. *Security integrity* definieras inte och tenderar att utifrån dagens terminologi verka aningen oklart och oprecist. *Data integrity* sägs inte vara relaterad till innehållet, däremot till *”inconsistency in the data structure”*.
Availability	3	Begreppsanvändningen är inte tydligt relaterad till nu aktuellt terminologibruk.

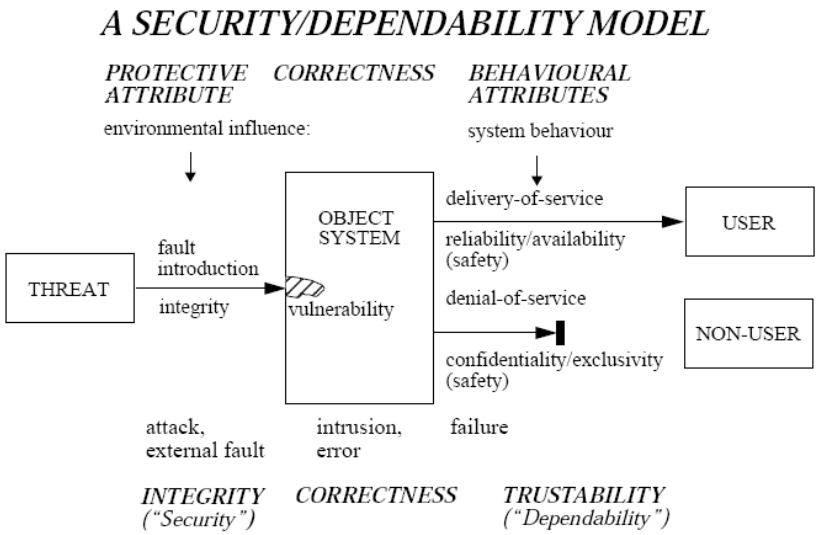
Enligt Fåk (2004) var det först framåt sent 80-tal som terminologibruket stabiliserade kring de nu nästintill självklara begreppen sekretess, riktighet och tillgänglighet. Gollmann (2011) påpekar problematiken med att det existerar olika definitioner av begreppet säkerhet (security) och att allt för mycket tid och resurser går åt till den svårlösta uppgiften att definiera en entydig begrepps-apparat. För de vidare resonemangen i denna rapport är det värdefullt att indikera några av dessa definitionsproblem.

Gollmann (2011) påpekar avseende sekretess (confidentiality) att begreppet kan relatera till skydd av persondata, vilket innebär avvägningar rörande personlig integritet (privacy), eller skydd av data relaterad till en organisation (secrecy). En betydande del av utvecklingen inom IT- och informationssäkerhet har tagit sin utgångspunkt i sekretessbehov och att sekretessbegreppet inte har någon motsvarighet inom problemdomänen fysisk säkerhet.

Gollmann (2011) påpekar avseende riktighet (integrity) svårigheten med att ge en koncis definition av begreppet. I korthet fokuserar begreppet på behov av att allt är som det förväntas vara, vilket inte är en definition som hjälper mycket, men den speglar verkligheten. Med något bättre precision kan riktighet beskrivas som behovet av skydd mot icke auktoriserat skrivande. Därmed blir riktighet i samband med policyer för informationsflöden en dual egenskap till sekretess. Samma tekniker kan då användas för att uppnå de båda skyddsmålen sekretess respektive riktighet. Om riktighet istället definieras som att hindra alla icke auktoriserade handlingar, så blir sekretess enligt (Gollmann, 2011) en del av

riktighetsbegreppet. Inom IT-säkerhet är definitionen av riktighet oftast begränsad till icke auktoriserade ändringar (skrivning), det vill säga manipulerande av data. Inom andra domäner av informationssäkerhet som telekommunikation inkluderas även slumpmässiga transmissionsfel, alltså icke aktörsdrivna ändringar.

Gollmann (2011) påpekar att grundproblemet avseende tillgänglighet uppstår när auktoriserade användares åtkomst till system och data förhindras eller begränsas i orimlig grad. Flertalet säkerhetsmekanismer för att nå detta skyddsmål hämtas, enligt Gollmann (2011) från andra discipliner än IT-säkerhet. Olika feltoleranta tekniker är exempel på tekniker som begränsar antagonisters möjligheter. Enligt Gollmann (2011) är tillgänglighet i många sammanhang sannolikt det viktigaste skyddsmålet, samtidigt som det finns en tydlig brist på säkerhetsmekanismer för att hantera tillgänglighetsrelaterade problem.



Figur 2 Integrerad modell avseende säkerhet (security) och driftsäkerhet (Jonsson, 2006).

Jonsson (1998 & 2006) diskuterar informationssäkerhetsområdets grundbegrepp och relaterar dessa till begreppsbildning inom driftsäkerhets- och tillförlitlighetsforskning. Gränsdragandet mellan säkerhet (security) och andra kritiska områden i sig är problematisk, då det inte är tillräckligt att säkra maximal sekretess, riktighet och tillgänglighet för att uppnå en tillfredsställande säkerhetsnivå (Sterne, 1991). Jonsson (2006) presenterar även en modell (Figur 2) för att integrera säkerhet (security) och driftsäkerhet. Brist på riktighet utgör i modellen en beskrivning av hur hot kan introducera miljöpåverkan på ett målsystem genom att via utnyttjande av en sårbarhet i målsystemet lyckas med ett intrång och

introducera ett fel i systemet, vilket innebär att systemet manipuleras. Intrång kan därmed innebära att systemet helt eller delvis fallerar i att leverera tjänster till sina användare. Tillgänglighet innebär i modellen ett systembeteende i form av att tjänsteleverans sker som förväntat till auktoriserade användare av mål-systemet.

Sekretess innebär i modellen att icke auktoriserad användare nekas tjänste-leverans i form av informationsleverans. Begreppet exklusivitet (exclusivity) innebär i modellen att icke auktoriserade användare nekas tjänsteleverans genom att de inte ges åtkomst till systemtjänster.

3 Två tänkta fall och ett grundproblem

I detta kapitel presenteras två tänkta fall som avses illustrera hur behoven av riktighet och tillgänglighet är tydliga och även samverkar med behoven av sekretess.

3.1 Säker kommunikation?

I ett tänkt fall finns det i ett låst utrymme en enhet för säkrare kommunikation via en krypterad länk. Enheten är markerad med en etikett som deklarerar att enheten har ett godkänt skydd mot röjande signaler (RöS).

För att komma in till enheten för säkrare kommunikation krävs först att dörrar med kortläsare passeras. Dörrarna är i trä och kan därmed forceras. Kommunikationsenheten är inte under kontinuerlig uppsyn och kontroll. Detta öppnar upp för att en illvillig individ kan säkra åtkomst till enheten för säkrare kommunikation, manipulera enhetens RÖS-skydd så att det inte fungerar som förväntat och därigenom möjliggöra åtkomst till kommunikationsenhetens informationsflöde. Balansen mellan tillgänglighet, riktighet och sekretess har därmed blivit påverkat på ett otillbörligt sätt. Manipulering medför att enhetens riktighet har påverkats, vilket möjliggör påverkan på sekretess. Etiketten om skydd mot RöS meddelar att skyddet har installerats, men huruvida det kvarstår och inte har manipulerats är inte lika enkelt att säkerställa.

Huruvida enskilda händelser i kedjan är svåra att genomföra bedöms inte närmare i denna rapport. Det är inte denna detaljproblematik som fokus är på. Däremot indikerar detta fall en komplexitet i sambanden mellan olika informationssäkerhetsegenskaper, säkerhetsmekanismer och eftersträvad säkerhetsnivå. Väl vald och designad kryptering är en särskilt sekretesshöjande mekanism, särskild om nyckelhanteringen är utformad på ett bra sätt. Dock, om en illegitim användare genom att forcera trädörrar kan säkra fysisk tillgång till kommunikationsenheten, åskådliggörs att tillgänglighet, riktighet och sekretess inte är oberoende egenskaper.

3.2 IT-system kontra tekniska system

I ett ytterligare tänkt fall har ett IT-baserat styrsystem utvecklats. Styrsystemet är efterfrågat och driftsättande av systemet närmar sig. Miljön där styrsystemet skall användas är helt beroende av styrsystemet för att kunna uppnå någon som helst funktionalitet. Ackreditering av styrsystemet, det vill säga godkännande för driftsättande av styrsystemet med en beskriven uppsättning av säkerhetsfunktioner, krävs ifall systemet anses vara ett IT-system.

Ackrediteringsprocessen är känd för att kräva betydande arbete och tid. Dessutom upplevs det vara en betydande osäkerhet kring huruvida ackrediteringen kommer leda fram till ett godkännande för driftsättande. Ackrediteringen tenderar att särskilt fokusera på olika säkerhetsfunktioner som bidrar till att sekretesskrav uppfylls.

I sammanhangen observeras följande:

1. IT-system kräver ackreditering.
2. Tekniska system kräver inte ackreditering.
3. Styrsystem kan anses vara tekniska system.
4. Ergo: Ackreditering av styrsystemet genomförs inte.

Därigenom möjliggörs grundläggande tillgänglighet avseende styrsystemet och att styrsystemet kan utnyttjas i förväntad utsträckning och inom önskad tid i den miljö i vilket styrsystemet används. Miljön i vilket styrsystemet används har därmed säkrat sin helt basala och grundläggande funktionalitet. Men en ackreditering har inte genomförts och därmed inte en granskning av styrsystemets säkerhetsfunktionalitet relativt sin miljö. Bristen på granskning innebär en brist på kännedom om säkerhetsnivå i allmänhet och även avseende riktighet. Om en illvillig aktör manipulerar styrsystemet, det vill säga påverkar riktigheten, så kan detta medföra att hela miljön i vilket styrsystemet ingår, inte fungerar som normalt. Det kan rent av agera rent kontraproduktivt. Med andra ord om inte riktighet kan säkras, påverkas även tillgängligheten och tänkbart även sekretessen.

3.3 Grundproblem

De två fallen i avsnitt 3.1 och 3.2 illustrerar en grundproblematik relaterad till informationssäkerhet. Sekretess, riktighet och tillgänglighet betraktas till betydande grad som oberoende aspekter med separata hanteringssätt. Detta synssätt är ofta det rådande i policyer, handböcker och andra styrande dokument.

Samtidigt illustrerar på ett enkelt sätt ovanstående fall att det finns påverkan och beroenden mellan informationssäkerhetsegenskaperna sekretess, riktighet och tillgänglighet. Om beroenden mellan informationssäkerhetsegenskaperna inte tydliggörs och effektivt hanteras, är detta presumtivt kritiskt och allvarligt för verksamheten, som är beroende av välfungerande IT-system. I båda dessa tänkta fall spelar riktigheten en viktig, men allt för ofta negligerad roll.

4 Perspektiv på informationssäkerhet inom Försvarsmakten

En vanligt förekommande *uppfattning* av hur informationssäkerhet betraktas inom Försvarsmakten (FM), är att sekretess är en dominerande och prioriterad egenskap. Resonemang i detta kapitel utmanar delvis denna bild genom att de olika perspektiv som finns inom Försvarsmaktens verksamhetsplanering respektive inom Försvarsmaktens operativa verksamhet beskrivs.

Detta kapitel är en sammanfattning av observationer ur och behovsbild identifierade i en av FOI tidigare genomförd intervjustudie. Observationerna och behovsbilden som redovisas relaterar till informationssäkerhetsegenskaperna sekretess, riktighet och tillgänglighet.

4.1 Avvägningar avseende sekretess, riktighet och tillgänglighet

Hunstad, Gustafsson, Karlzén, Mörnestedt och Westerdahl (2012) redovisar intervjuer genomförda under maj 2012 med respondenter inom FM och FMV avseende dagens och framtidens informationssäkerhetsbehov inom Försvarsmakten. Respondenterna vid denna intervjuserie representerade olika intressenter i form av produkt- och systemägare, beställningsansvariga, upphandlingsansvariga, arbetande inom operativt underrättelsearbete och operativt militärt arbete. Detta avsnitt sammanfattar intervjustudiens observationer där dessa bedöms vara av relevans för denna studie.

Vid denna intervjuserie framkom synpunkter på att det är svårt att göra avvägningar mellan tillgänglighet och sekretess. Sekretessnivån är i många Försvarsmaktssammanhang gränssättande. Ur ett tillgänglighetsperspektiv uppstår problem när information hålls otillgänglig en period, varvid sekretessen prioriteras. Förfarandet kan bero på bedömningar att arbetsdokument inte bör spridas, ty de kan vara otillräckliga eller vilseledande för läsaren eftersom slutversionen kan bli annorlunda. Samtidigt pågår en utveckling för en ökad användarvänlighet och därmed blir tillgänglighet en allt viktigare aspekt för IT-system.

Mycket skydd läggs för närvarande på en liten, men särskild skyddsvärd del av informationen. Samtidigt läggs små resurser på skydd av den övriga stora mängden mindre skyddsvärd information. Även den kan kräva visst skydd, ty information som i strikt mening inte omfattas av sekretess, samtidigt inte bör spridas fritt. Omfattande aggregat av information kan också bli mer skyddsvärda än enskilda beståndsdelar.

I Försvarsmaktens säkerhetsarbete har, enligt yttranden ur intervjustudien i (Hunstad, Gustafsson, Karlzén, Mörnestedt, & Westerdahl, 2012), riktighet som informationssäkerhetsegenskap inte varit i fokus. Samtidigt är tillgång till korrekt information kritiskt i strid där det inte finns tid till att åtgärda brister i informationen. Riktighet är också kritiskt avseende autentisering för att kunna avgöra om användare och system är vilka de påstår. Denna problematik indikerar även vikten av spårbarhet för att kunna utkräva ansvar.

4.2 Behovsbild

Analysen av den i avsnitt 4.1 omnämnda intervjuseriens intervjuunderlag identifierade behovsrelaterade skillnader mellan verksamhetsplanering och operativ verksamhet inom Försvarsmakten (Hunstad, Gustafsson, Karlzén, Mörnestedt, & Westerdahl, 2012). Av dessa behovsrelaterade skillnader är vissa direkt relaterade till avvägningar kring olika informationssäkerhetsegenskaper:

- *Sekretessbelagd information* – spelar en avgränsad roll i fält, men kan vara av central vikt vid verksamhetsplanering.
- *Riktighet kontra sekretess* – i fält är riktighet av större vikt än sekretess. Likaså är det i fält av stor vikt att information är aktuell, vilket innebär behov av inhämtning av information. Vid verksamhetsplanering har sekretess större vikt.

Ytterligare behovsrelaterade skillnader handlar mer om säkerhetsavvägningar i allmänhet:

- *Enkelhet och robusthet kontra säkerhet* – fältmässiga situationer präglas av behov av enkelhet och robusthet medan verksamhetsplaneringsnivån främst har behov av säkerhet.
- *Skydd och verkan* – säkerhetsfokus vid verksamhetsplanering medför skyddsbehov medan verkan kan tvingas gå före skydd vid operativ verksamhet.
- *Riskvärdering* – i fält behövs robusta metoder för riskvärdering och med tanke på tidsbrist är automatiserade metoder av intresse. Verksamhetsplanering präglas däremot inte av samma tidskritiska perspektiv avseende riskvärdering.

Tre ytterligare behovsrelaterade skillnader pekar på faktorer som beskriver miljöskillnader:

- *Tidsperspektiv* – operativ verksamhet kräver snabba beslut och agerande medan verksamhetsplanering har längre tidsperspektiv.

- *Mobilitet* – militär operativ verksamhet ställer betydande krav på mobilitet, vilket inte verksamhetsplanering gör på samma sätt.
- *Hantering av större informationsmängder* – vid verksamhetsplanering finns normalt mer omfattande datorresurser och datamängder att hantera, medan operativ verksamhet har större behov av snabba beräkningar och beslut.

5 Styrande dokument

Detta kapitel redovisar ett urval av Försvarsmaktens styrande dokument relaterade till informationssäkerhet. Fokus i redovisningen är på hur informationssäkerhetsegenskaperna sekretess, riktighet och tillgänglighet får olika utrymme i dokumenten och möjligtvis medför olika påverkan inom Försvarsmaktens verksamhetsplanering och operativa verksamhet.

5.1 H Säk Infosäk

Handbok Försvarsmaktens säkerhetstjänst, Informationssäkerhet (H Säk Infosäk) vänder sig primärt till Försvarsmaktspersonal som direkt skall stödja Försvarsmaktens informationssäkerhetsarbete snarare än till de som hanterar informationstillgångarna (Försvarsmakten, 2013). Författningar som reglerar informationssäkerheten förklaras, liksom Försvarsmaktens uppfattning om hur föreskrifter om säkerhetsskydd skall tillämpas redovisas i handboken.

Enligt handboken, såsom definierad av Försvarsmaktens informationssäkerhets-policy, avses med informationssäkerhet i Försvarsmakten att:

- informationen finns tillgänglig när den behövs
- informationen är och förblir riktig
- informationen endast är tillgänglig för dem som är behöriga att ta del av och använda den
- hanteringen av informationen är spårbar.

Som en synnerligen förenklad mätning på viktläggningen av olika informations-säkerhetsegenskaper i H Säk Infosäk räknades antal träffar i dokumentet på de ord som beskriver de primära informationssäkerhetsegenskaperna[4]. I antalet träffar räknas alla träffar in på sökordet inklusive böjningar och sammanskrivningar med andra termer. Utfallet av denna enkla mätning är följande:

[4] Här även inräknat termen konfidentialitet som vid ett vägval tidigt i rapportens diskurs tilldelades en i själva resonemanget avgränsad roll.

Informations-säkerhetsaspekt	Antal träffar i (Försvarsmakten, 2013)
Konfidentialitet	3
Sekretess	894
Riktighet	12
Tillgänglighet	29

I och med att andra termer ibland används istället för termen riktighet genomfördes även ytterligare sökningar på termerna korrekthet och integritet. Detta resulterade i noll träffar för korrekthet respektive 4 för integritet. Avseende termen integritet bedöms användandet av denna i handboken inte beröra den informationssäkerhetsrelaterade termen riktighet. Mätningen indikerar ett volymmässigt fokus i H Säk Infosäk på sekretess gentemot de två övriga informationssäkerhetsegenskaperna. Vissa kompletterande reflektioner rörande H Säk Infosäk och särskilt dess relation till Säkerhetsskyddslagen, redovisas i avsnitt 5.3.

5.2 Krav på säkerhetsfunktioner (KSF)

Bengtsson, Sommestad och Holm (2014) redovisar två studier kopplade till Försvarsmaktens *Krav på Säkerhetsfunktioner KSF3* (Försvarsmakten, 2014). En av dessa studier konstaterar att KSF3 innehåller krav som syftar till att hantera risken kopplat till att en händelse påverkar sekretessen för den information som systemet hanterar. Därmed kan det observeras att KSF inte fokuserar på de två övriga primära informationssäkerhetsegenskaperna riktighet respektive tillgänglighet. Ej heller spårbarhet, vilket också är en aspekt av vikt, är i fokus i KSF3.

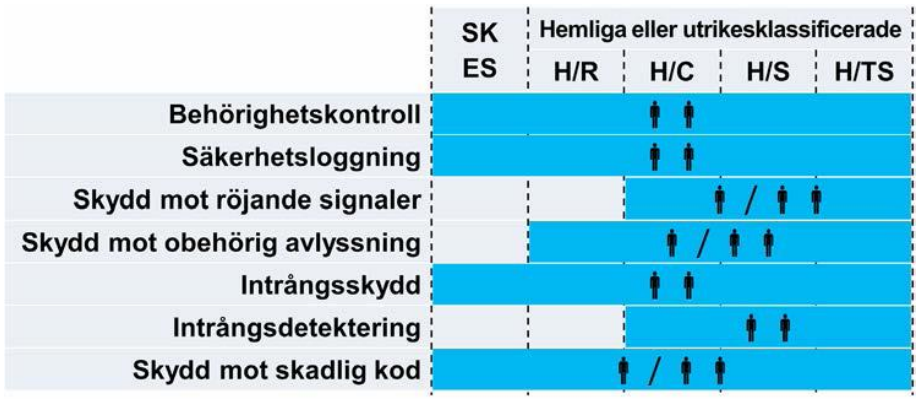
KSF3:s fokus på sekretess innebär dock inte att alla krav på riktighet, tillgänglighet respektive spårbarhet är förbisedda. Dels finns det KSF3-krav som är direkt relaterade till riktighet och spårbarhet, dels bidrar många realiserade säkerhetslösningar till flera av informationssäkerhetsegenskaperna. KSF3-krav på riktighet finns bland annat avseende konfigurationer, mjukvaror och meddelanden. Avseende spårbarhet finns krav på loggar och oavvislighet.

KSF3 förutsätter att ytterligare krav än de inom KSF3 definierade kan behövas. Dessa benämns som tillkommande säkerhetskrav och förutsätts bli identifierade genom verksamhets- och säkerhetsanalyser. Bengtsson, Sommestad och Holm (2014) ser det som rimligt att en betydande del av de tillkommande kraven kommer att fokusera på att möta hot mot riktighet, tillgänglighet och spårbarhet. En genomgång av modeller och teorier redovisade i vetenskaplig litteratur visar dock på begränsade möjligheter för utökning av KSF. Inom litteratur avseende

tillgänglighet saknas det antagonistiska perspektiv som karakteriserar informationssäkerhet. Avseende riktighet bedömer Bengtsson, Sommestad och Holm (2014) att det är svårt att inom litteraturen identifiera bidrag eller idéer med fokus på tillkommande riktighetskrav. Slutligen bedöms existerande IT-forensiska teorier och modeller inte relatera till KSF3:s abstraktionsnivå.

5.3 Säkerhetsskyddslagen, säkerhetsskyddsförordningen och relationen till KSF

Säkerhetsskyddslagen och säkerhetsskyddsförordningen innehåller grundläggande föreskrifter om hur information som rör rikets säkerhet skall skyddas och fokuserar därmed på hemliga uppgifter.



Figur 3 Säkerhetsfunktioner som skall finnas i ett IT-system i Försvarsmakten beroende på uppgifter systemet avses behandla respektive huruvida systemet avses användas av en (markerat med 🧍) eller flera personer (markerat med 🧍🧍). ES: Ej sekretess enligt offentlighets- och sekretesslagen. SK: Sekretessklassificerade uppgifter (Försvarsmakten, 2013).

I enlighet med Försvarsmakten och Säkerhetspolisens definition, så som redovisat i H Säk Infosäk (Försvarsmakten, 2013), existerar det sju säkerhetsfunktioner för de IT-system som är avsedda för behandling av hemliga uppgifter:

- behörighetskontroll
- säkerhetsloggning
- skydd mot röjande signaler
- skydd mot obehörig avlyssning

- intrångsskydd
- intrångsdetektering
- skydd mot skadlig kod.

Vilka säkerhetsfunktioner som skall finnas i ett IT-system i Försvarsmakten beror på vilka uppgifter systemet avses behandla, respektive huruvida systemet är ett en- eller fleranvändarsystem (figur 3). Försvarsmakten (2013) klargör vidare att tillräcklig IT-säkerhet inte enbart kan uppnås med de sju säkerhetsfunktionerna. Säkerhetsfunktionerna definierar inte alla nödvändiga skyddsåtgärder, vilket leder fram till behov av säkerhetsanalys där tillkommande säkerhetskrav kan identifieras.

KSF:s krav berör alla uppgifter som behandlas inom IT-systemen, inte endast uppgifter rörande rikets säkerhet (Hakkarainen, 2016). Tre kravnivåer är specificerade (grund, utökad och hög), vilka relateras till konsekvensnivå vid informationsförlust respektive exponeringsnivå mot aktörer som kan påverka systemet.

I och med att KSF berör alla uppgifter som behandlas inom IT-systemen och inte endast de uppgifter som berör rikets säkerhet, uppstår delikata och komplexa avvägningar. Avseende krav på IT-säkerhetsförmåga har Försvarsmakten, enligt Hakkarainen (2016), likställt säkerhetsskyddet (det vill säga skydd av information som berör rikets säkerhet) med IT-säkerhetsskydd för uppgifter som inte omfattas av sekretess enligt offentlighets- och sekretesslagen. Detta är en i sig intressant problematik som dock här endast kort omnämns för att indikera en ytterligare utmaning relaterad till hantering av informationssäkerhet. Utmaningen handlar mycket om svårigheten att identifiera adekvata begrepp och relatera bruken och en praktisk innebörd av dessa begrepp till en oerhört komplex verksamhet och verklighet. Dessutom berör denna problematik i huvudsak sekretess, och denna rapport försöker att primärt lyfta fram hur andra informationssäkerhetsegenskaper än sekretess hanteras inom Försvarsmakten.

Betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25) skall svara mot förändrade krav på säkerhetsskydd, bland annat avseende IT-utvecklingen. Betydelsen av riktighet och tillgänglighet hos information och informationssystem accentueras.

I betänkandets avsnitt om riktighet och tillgänglighet föreslås att *”informationssäkerheten ska förebygga skadlig inverkan på sådana uppgifter”*[5]. Existerande definitioner av informationssäkerhet listar i allmänhet sekretess, riktighet och tillgänglighet som i begreppet informationssäkerhet ingående egenskaper. Ur perspektivet av att förhålla sig till definitioner av informationssäkerhet

[5] Ur kontexten framgår att med uttrycket *”sådana uppgifter”* avses uppgifter där riktighet och tillgänglighet är av vikt.

formulerar därmed betänkandet en självklarhet. Ur ett annat perspektiv kan betänkandet möjligen formulera ett önskemål och behov av att praktiskt arbete inom informationssäkerhet i högre grad skall förebygga skadlig inverkan på riktighet och tillgänglighet. Samtidigt redovisar betänkandet reflektioner kring att riktighets- och tillgänglighetskrav sägs vara svårare att indela i nivåer än sekretesskrav, vilket vidare sägs bero på att kraven kan vara mycket varierande i olika verksamheter och system och även svårare att uttrycka i generella termer.

Ovanstående indikerar en problematik med att med utgångspunkt i säkerhetsskyddslagen och definitioner av informationssäkerhet utveckla relevanta och adekvata informationssäkerhetsarbetsrutiner som täcker olika aspekter av informationssäkerhet. För betänkandet om ny säkerhetsskyddslag kan det vidare noteras att uppdraget formulerades utifrån behov av att tydligt väga in betydelsen av att tillhandahålla krav på riktighet och tillgänglighet. Betänkandet redovisar inte krav eller tydliga vägar vidare för att hantera informations-säkerhetsegenskaperna riktighet och tillgänglighet. Hakkarainen (2016) pekar på möjligheten att myndigheter med föreskriftsrätt inom säkerhetsskyddsområdet föreskriver om klassificeringsbegrepp för riktighet och tillgänglighet. Vidare argumenterar han för att använda olika klassificeringsbegrepp för säkerhets-skyddsklassificerade respektive andra uppgifter. Detta för att hantera adekvata skyddsnivåer avseende riktighet och tillgänglighet för uppgifter rörande rikets säkerhet relativt uppgifter som inte är av denna art, vilket motsvarar ovan indikerade tankesätt avseende sekretess.

6 Diskussion och slutsatser

Försvarsmakten har en stark sekretesstradition, vilket inte är unikt för Försvarsmakten. Även inom många andra organisationer existerar sådana traditioner. Gollmann (2011) påpekar att en betydande del av utvecklingen inom IT- och informationssäkerhet har tagit sin utgångspunkt i sekretessbehov, vilket medför att sekretess har varit den dominerande aspekten.

Försvarsmaktens sekretesstradition har sannolikt sitt ursprung långt tillbaka innan strikta definitioner av begrepp formulerades, då IT- och informationssäkerhet var okända företeelser. Genom civilisationens historia har människan på olika sätt förvaltat och lagrat information. Forntida skriftsystem var i sig sannolikt sekretessbevarande, ty få kunde läsa och skriva. Människans behov av information har under historiens gång medfört att praxis har utvecklats avseende informationshantering, till exempel i form av tidiga krypteringsvarianter som exempelvis Caesarkryptot. Detta har inneburit restriktioner på hur information har fått hanteras, och rimligen har särskilda och starka behov funnits inom militära sammanhang. Successivt har även mer explicita krav ställts på informationshantering.

Vid samtal med seniora säkerhetsexperter vid FOI lyftes tanken att reflektioner kring riktighet och tillgänglighet i informationssäkerhetsmässig mening kan ha fått ett tydligare utrymme i Försvarsmaktssammanhang sedan ett fåtal år bakåt. Detta kan indikera en potential för framtida utveckling.

De i kapitel 3 beskrivna fallen implicerar, tillsammans med resonemang kring begreppsutvecklingen inom informationssäkerhet i kapitel 2, vikten av att sammanväga behov såväl på sekretess och riktighet som på tillgänglighet. Kravutveckling och specificerande av säkerhetsmekanismer bör i större grad ta sin utgångspunkt i sådana gemensamma och sammanvägda behov. I en sådan utvecklingsprocess, med sikte på Försvarsmaktens behov, är det eftersträvansvärt att tydliga hänsyn tas till olika behovsbilder för verksamhetsplanering respektive operativ verksamhet med sina olika prioriteringar avseende sekretess, riktighet och tillgänglighet.

Nuvarande utformning av, för Försvarsmakten centrala, styrande dokument avseende informationssäkerhet, indikerar också behov och potential för vidare utveckling där riktighets- och tillgänglighetsaspekterna på ett tydligare och bättre sätt bidrar. Samtidigt bör det nyktert observeras att de centrala styrande dokumentens utformning har en parallell i den allmänna begreppsutvecklingen inom informationssäkerhet. I båda fallen har sekretessbehoven varit relativt dominerande som drivkraft. Eventuellt är denna drivkraft mer accentuerad i Försvarsmaktssammanhang.

En tänkbar modell att ta utgångspunkt i vid fortsatt arbete, för att hitta en förbättrad balans mellan de centrala informationssäkerhetsegenskaperna, kan vara den integrerade modell avseende säkerhet (security) och driftsäkerhet som presenteras i slutet av kapitel 2. Modellen åskådliggör relationer mellan centrala informationssäkerhetsegenskaper, extern systempåverkan respektive tjänsteleveranser.

Något som också måste beaktas är att informationssäkerhet skall motsvara de behov som finns inom aktuell organisation. Detta medför att balansen mellan de tre aspekterna och även deras absoluta betydelse beror på vilka behoven av informationssäkerhet (och dess olika egenskaper) som finns. Ett sätt att belysa dessa behov ges av säkerhetsanalyser och även vidare analyser av informationssäkerhetsrisker, vilka visar på vilka risker kopplade till informationssäkerheten som behöver hanteras. Kopplat till detta är det också väsentligt att åskådliggöra vilken nytta som uppnås med olika informationssystem och -tjänster så att avvägningar mellan nytta och risker kan göras.

7 Referenser

Anderson, J. (1972). *Computer security technology planning study.* U.S. Air Force Electronic Systems Technical Report. Hämtat från http://csrc.nist.gov/publications/history/ande72.pdf

Bengtsson, J., Sommestad, T., & Holm, H. (2014). *IT-säkerhetskrav i Försvarsmakten - KSF3 och tillkommande säkerhetskrav.* Totalförsvarets forskningsinstitut (FOI).

Fåk, V. (2004). *Datasäkerhet, kompendium.* Linköpings universitet.

Försvarsmakten. (2013). *Handbok Säkerhetstjänst Informationssäkerhet H Säk Infosäk.* Försvarsmakten.

Försvarsmakten. (2014). *KSF: Krav på IT-säkerhetsförmågor hos IT-system, v3.1.* Försvarsmakten.

Gollmann, D. (2011). *Computer Security* (Third edition uppl.). John Wiley & Sons, Ltd.

Hakkarainen, K. (2016). Kim Hakkarainen, Blogg om informationssäkerhet. Hämtat från http://blogg.mrpoyz.net/gemensamma-skyddsnivaer/

Hunstad, A. G., Gustafsson, T., Karlzén, H., Mörnestedt, F., & Westerdahl, L. (2012). *Objektbaserad säkerhet - Behov och möjligheter.* Totalförsvarets forskningsinstitut (FOI).

Jonsson, E. (1998). An Integrated Framework for Security and Dependability. *NSPW '98 Proceedings of the 1998 workshop on New security paradigms* (ss. 22-29). Charlottesville, Virginia, USA: ACM.

Jonsson, E. (2006). Towards an Integrated Conceptual Model of Security and Dependability. *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)* (ss. 219-230). IEEE. Hämtat från http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1625369

SIS. (2007). *SIS HB 550: Terminologi för informationssäkerhet, utgåva 3.*

SIS. (2015). *Terminologi för informationssäkerhet.* Teknisk rapport.

SOU 2015:25. (u.d.). *En ny säkerhetsskyddslag.* Hämtat från http://www.regeringen.se/contentassets/08d4b02afbc348edad916de817105a9c/en-ny-sakerhetsskyddslag-sou-201525

Sterne, F. (1991). On the Buzzword Security Policy. *IEEE Symposium on Security & Privacy.* IEEE. Hämtat från http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=130789

Ware, W. H. (1970). *Security controls for computer systems* . Santa Monica, CA: The RAND Corporation. Hämtat från http://www.rand.org/pubs/reports/R609-1/index2.html

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