Beskrivning av hot vid säkerhetsanalyser

Innehåll och utformning

Jonas Hallberg, Johan Bengtsson, Henrik Karlzén

FOI-R--4676--SE

December 2018

FOI

Jonas Hallberg, Johan Bengtsson, Henrik Karlzén

Beskrivning av hot vid säkerhetsanalyser

Innehåll och utformning

Bild/Cover: Johan Bengtsson

Titel	Beskrivning av hot vid säkerhetsanalyser – Innehåll och utformning
Title	The description of threats in risk analyses – Content and phrasing
Rapportnr/Report no	FOI-R--4676--SE
Månad/Month	December
Utgivningsår/Year	2018
Antal sidor/Pages	53
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation Cyber
FoT-område	E72728
Projektnr/Project no	Christian Jönsson
Godkänd av/Approved by	Ledningssystem
Ansvarig avdelning	Innehållet är granskat och omfattar ingen information
Exportkontroll	som är underställd exportkontrollagstiftningen.

Sammanfattning

Att bedöma sannolikheter och konsekvenser är en central del i genomförandet av säkerhetsanalyser inom Försvarsmakten. Vid systematiskt arbete med säkerhetsanalyser ligger skriftliga beskrivningar av identifierade hot till grund för dessa bedömningar. Det saknas dock till stor del kunskap om hur dessa hotbeskrivningars innehåll och utformning påverkar bedömningarna av sannolikhet och konsekvens.

För att stödja framtagandet av hotbeskrivningar som utgör adekvat underlag för riskbedömningar presenteras i denna rapport ett förslag avseende vad en hotbeskrivning ska innehålla och hur den ska utformas. Till grund för innehållet presenteras en uppsättning med informationselement som ska ingå i en hotbeskrivning. Till stöd för utformningen av hotbeskrivningar presenteras även en uppsättning med principer som bör följas. Förslaget är inte avsett att utgöra en slutlig version utan ska beaktas som en utgångspunkt för vidare diskussion och utveckling av kunskapen om vad som behöver ingå i en hotbeskrivning och hur den ska utformas.

Som ett första steg i att utvärdera den föreslagna uppsättningen informationselement som utgör en hotbeskrivning genomfördes en kvantitativ enkätstudie. Studien utformades för att undersöka vilken påverkan specificeringen av aktör har på bedömningen av sannolikhet och konsekvens för ett hot. Resultaten från studien visar bland annat att det finns en stor variation mellan olika respondenter med avseende på hur de bedömer sannolikhet och konsekvens utgående från identiska hotbeskrivningar.

Nyckelord: risk, informationssäkerhet, sannolikhet, konsekvens

Summary

The assessment of probabilities and consequences is fundamental for the specification of information security risks. In structured risk assessments, written descriptions of the identified threats constitute the basis for these assessments. However, there is currently insufficient knowledge regarding how the content and phrasing of threat descriptions affects the assessment of the probability and the consequence.

To support the production of adequate threat descriptions, a proposal concerning the content and phrasing of threat descriptions is presented. As the basis for specifying the content, a set of information elements to be included in threat descriptions is presented. To support the phrasing of threat descriptions, a set of principles to be adhered to is presented. The proposal is not to be considered as final but rather as a starting point for discussions and further development of the knowledge considering what to be included in threat descriptions and how to phrase them.

As a first step in assessing the proposal concerning the content of threat descriptions, a quantitative survey-based study was performed. The study was designed in order to investigate whether the specification of the actor has any influence on the assessment of the probability and the consequence. The results of the study show, among other things, that there are large variations between the respondents regarding their assessments of probability and consequence.

Keywords: risk, information security, probability, consequence

Innehåll

1 Inledning

Inom Försvarsmakten ska säkerhetsanalyser genomföras för att identifiera alla skyddsvärda tillgångar vilkas påverkan av oönskade händelser medför negativa konsekvenser för verksamheten. Analyserna ska genomföras för flera olika typer av verksamheter, exempelvis innan nya IT-system införs. Inom Försvarsmakten genomförs analyserna enligt metoden för säkerhetsanalys som beskrivs i H Säk Grunder. Säkerhetsanalyserna genomförs för att identifiera och specificera ett antal faktorer som ska ligga till grund för bedömningen av sannolikhet och konsekvens för varje identifierat hot. Vilken betydelse har de resulterande skriftliga beskrivningarna av identifierade hot för bedömningen av sannolikhet och konsekvens? Idealt skulle det finnas kunskap om vad som ska ingå i en hotbeskrivning och hur denna information ska presenteras i skrift för att på bästa sätt stödja riskbedömningen. Tyvärr finns det få studier som belyser denna fråga och det finns många frågeställningar som behöver formuleras och besvaras för att få fram denna kunskap.

Det finns många olika uppslag till metoder och arbetssätt som ger en struktur för hur arbetet med identifiering av hot ska gå till. Försvarsmakten har flera handböcker som beskriver hur detta arbete ska genomföras för Försvarsmaktens verksamheter, exempelvis H Säk Grunder (Försvarsmakten, 2013), H Säk Hot (Försvarsmakten, 2006) och H Säk IT Hot (Försvarsmakten, 2001). Ett viktigt moment, som dock inte beskrivs i någon av handböckerna, är hur de identifierade hoten ska beskrivas i skrift när resultaten ska dokumenteras. Det kan tyckas som att den viktiga delen av arbetet är genomförd när hoten har identifierats, men om inte hoten beskrivs på ett tydligt sätt i en hotbeskrivning kan de vara både svåra att förstå och bedöma i det fortsatta arbetet.

I denna rapport presenteras ett förslag på vilken information som ska ingå i en hotbeskrivning för att den ska utgöra ett adekvat underlag vid bedömning av sannolikhet och konsekvens för det aktuella hotet. Förslaget består av två delar som relaterar till innehållet i respektive utformningen av hotbeskrivningar. Informationen som behöver ingå i en hotbeskrivning delas upp i flera informationselement som tillsammans utgör en hotbeskrivning. Stöd för hur hotbeskrivningar ska formuleras i skrift ges genom ett antal principer för utformningen av hotbeskrivningar. Syftet med förslaget är att skapa en utgångspunkt för fortsatta studier med att identifiera hur informationen i hotbeskrivningar påverkar de bedömningar som görs under en säkerhetsanalys samt hur stödet för framtagandet av hotbeskrivningar kan utvecklas.

Som ett första steg i att undersöka hur informationen i hotbeskrivningarna påverkar bedömningarna av sannolikhet och konsekvens för ett hot har en

enkätstudie genomförts. Enkätstudien utformades för att undersöka hur specificeringen av aktör[1] påverkar bedömningarna.

I kapitel 2 beskrivs det innehåll som är nödvändigt i en hotbeskrivning utgående från Försvarsmaktens handböcker inom området. Jämförelser görs även med vad som föreslås i olika standarder och riskanalysmetoder. I kapitel 3 beskrivs hur hotbeskrivningar ska utformas i skrift. Utgångspunkten är åtta principer som används vid kravspecificering, som är ett område med många likheter. I kapitel 4 presenteras, utgående från resultaten i kapitel 2 och kapitel 3, ett förslag till vilket innehåll som bör ingå i en hotbeskrivning samt vilka principer som bör följas när hotbeskrivningar utformas. I kapitel 5 beskrivs en enkätstudie som genomförts i syfte att undersöka hur specificeringen av aktör påverkar bedömningen av sannolikhet och konsekvens för ett hot. Avslutningsvis diskuteras resultaten i kapitel 6.

[1] Den som ger upphov till att ett hot kan realiseras.

2 Hotbeskrivningens innehåll

Idealt skulle hotbeskrivningar som utgör underlag för bedömning av risker innehålla all information som är nödvändig för riskbedömningen och ge full spårbarhet för på vilka grunder bedömningarna har gjorts. I praktiken måste dock avgränsningar göras för vilken information som kan finnas med i hotbeskrivningen och vilken detaljeringsgrad informationen kan ha. I detta kapitel beskrivs och diskuteras vilken information som hotbeskrivningen bör innehålla för att utgöra ett adekvat underlag för bedömning av risker.

Försvarsmaktens metodbeskrivning för säkerhetsanalyser som återfinns i H Säk Grunder (Försvarsmakten, 2013) användes som utgångspunkt för arbetet med att identifiera nödvändigt innehåll i en hotbeskrivning. Informationen som behöver ingå i en hotbeskrivning antas bestå av flera olika informationselement som tillsammans utgör en hotbeskrivning. En genomgång av metodbeskrivningen identifierade följande informationselement som nödvändiga i en hotbeskrivning: *tillgång, oönskad händelse, konsekvensbeskrivning, aktör, sårbarhet* och *existerande skyddsåtgärd*.

Under 2016 genomfördes på FOI en studie där det föreslogs att *tillvägagångssätt* läggs till som ett eget informationselement för att tydliggöra skillnaden mellan vad som beskriver en oönskad händelse och vad som beskriver det tillvägagångssätt som leder fram till att den oönskade händelsen inträffar (Hallberg, Bengtsson och Karlzén, 2016). Uppdelningen resulterar i en oönskad händelse som enbart berör den specificerade tillgången och som har samma konsekvensbeskrivning och konsekvensbedömning oavsett tillvägagångssätt. Specificeringen av tillvägagångssätten utgör underlag för kommande arbete med att identifiera sårbarheter och sannolikhetsbedömningen samt, vid behov, nödvändiga tillkommande skyddsåtgärder. I tabell 3 illustreras hur användandet av både informationselementen oönskad händelse och tillvägagångssätt kan se ut.

Tabell 1: Exempel på tänkt användning av informationselementen *oönskad händelse* och *tillvägagångssätt* (Hallberg, Bengtsson och Karlzén, 2016) baserat på exempel i H Säk Grunder (Försvarsmakten, 2013).

Tillgång	**Oönskad händelse**	**Tillväga-gångssätt**	**Konsekvens-beskrivning**	**Konsekvens-bedömning**
Dator-utrustning i lektionssal	Förlust av dator-utrustning	Inbrott i dator-lektionssal	Värdet på utrustningen uppgår till 500 kkr. Vid förlust kommer införandet av det nya verksamhetsledningssystemet att försenas med ca 6 månader.	4
		Brand i dator-lektionssal		
		Över-svämning i dator-lektionssal		

I syfte att undersöka om en hotbeskrivning bestående av informationselementen från H Säk Grunder kompletterat med ett separat informationselement för tillvägagångssätt är tillräckligt, gjordes en jämförelse med väletablerade standarder och metoder som används inom informationssäkerhetsområdet. De analyserade standarderna och metoderna identifierades via två studier genomförda av Korman m.fl. (2014) och Fenz m.fl. (2014). Under genomgången jämfördes informationselementen i den föreslagna uppsättningen med informationselement som extraherades från standarderna och metoderna. I den första kolumnen i Tabell 2 återges informationselementen från den föreslagna uppsättningen medan motsvarande informationselement från de olika standarderna och metoderna återges i kolumn två till fem. I många fall saknas exakt matchning mellan de föreslagna informationselementen och de informationselement som används i standarderna och metoderna. Ofta är informationselementen i standarderna och metoderna bredare än de föreslagna. För samtliga föreslagna informationselement finns motsvarande informationselement i flera av standarderna och metoderna. Detta indikerar att den föreslagna uppsättningen utgör en rimlig utgångspunkt för vad som ska ingå i hotbeskrivningar. I följande delavsnitt beskrivs och diskuteras de föreslagna informationselementen närmare.

Tabell 2: Föreslagen uppsättning med delar som ska ingå i hotbeskrivningar (Försvarsmakten, 2013; Hallberg, Bengtsson och Karlzén, 2016). Standarderna ISO/IEC 27005 (ISO/IEC, 2011), NIST Special Publication 800-30 Revision 1 (NIST, 2012), OCTAVE (Alberts och Dorofee, 2001) och Margerit 3.0 (Ministry of Finance and Public Administration, 2014).

Föreslagen uppsättning	**ISO/IEC 27005**	**NIST SP 800-30**	**OCTAVE**	**Magerit 3.0**
Tillgång	Information asset, Business process	Asset, Organizational operation	Asset	Asset
Oönskad händelse	Information security event		Outcome	Asset dimensions
Konsekvens-beskrivning	Impact criteria	Impact	Impact of threat	Impact of threat
Aktör	Origin of threat	Threat source	Source of threat	
Tillvägagångs-sätt	Incident scenario	Threat event	Access	
Sårbarhet	Vulnerability	Vulnerability	Vulnerability	Vulnerability
Skyddsåtgärd	Existing control	Security control		Safeguard

2.1 Tillgång

Generellt sett utgörs tillgångar av allt som är av värde för, exempelvis, en organisation. Tillgångarna är centrala när risker ska bedömas och utgör ofta det informationselement som ligger till grund för identifiering av de hot som ska bedömas. Försvarsmaktens metod för säkerhetsanalys använder tillgångar som utgångspunkten för analysarbetet. Det skiljs dock på *tillgångar* och *skyddsvärda tillgångar* där de sistnämnda är den delmängd av organisationens tillgångar som anses ha ett särskilt värde. Det är de skyddsvärda tillgångarna som ska beaktas när analyser görs enligt metoden för säkerhetsanalys. I H Säk Grunder påpekas att en rätt genomförd verksamhetsanalys bör resultera i att de skyddsvärda tillgångarna redan är identifierade. Oavsett om de skyddsvärda tillgångarna identifieras i verksamhetsanalysen eller under säkerhetsanalysen är svårigheten att hitta rätt avgränsningar för vad som är att betrakta som tillgångar och när de är skyddsvärda.

Ett stöd i att identifiera vad som kan utgöra tillgångar är att utgå från en befintlig kategorisering som beskriver olika typer av tillgångar. En kategorisering kan hjälpa till att vidga perspektivet för vad som kan utgöra tillgångarna i den aktuella organisationen. Försvarsmaktens förslag på kategorisering som återfinns i H Säk Grunder är att dela in skyddsvärda tillgångar i kategorierna:

- personal
- materiel
- information
- anläggningar
- verksamhet.

Ett alternativt förslag återfinns i den spanska metodiken MAGERIT (Ministerio de Administraciones Públicas, 2006) som istället föreslår att tillgångar delas in i kategorierna[2]:

- tjänster
- data
- mjukvaror
- datorutrustning
- kommunikationsnätverk
- media
- stödutrustning
- installationer
- personal.

SIS har under flera år bidragit till utvecklingen av svensk terminologi för informationssäkerhet. Den senaste utgåvan är SIS TR 50:2015[3] som ger stöd i identifieringen av tillgångar, specifikt informationstillgångar. Skriften ger följande exempel på hur informationstillgångar kan kategoriseras:

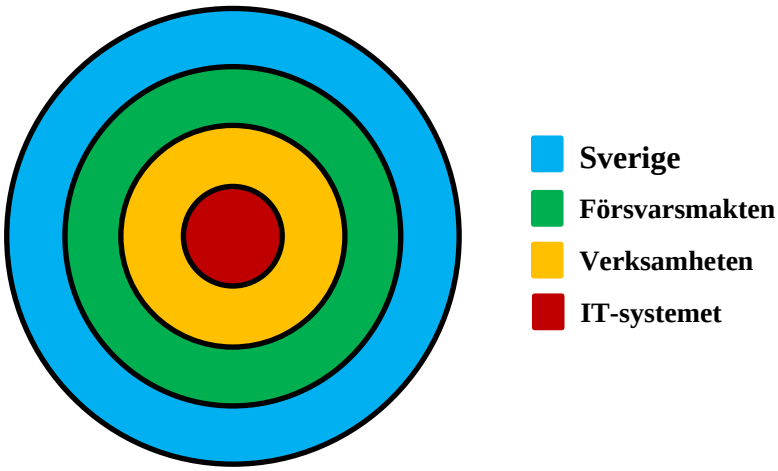
- information
- program
- tjänster

[2] Översatta från engelska.
[3] Teknisk rapport som har ersatt SIS Handbok 550, Utgåva 3 från 2007.

- fysiska tillgångar
- människor och deras kompetens, färdigheter och erfarenheter
- immateriella tillgångar.

Det finns följaktligen ett antal olika kategoriseringar av tillgångar att utgå ifrån när de skyddsvärda tillgångarna ska identifieras i en säkerhetsanalys, men det finns otydligheter. Exempelvis är verksamhet en av tillgångskategorierna i H Säk Grunder, samtidigt som oönskade händelser är något som påverkar tillgångar och resulterar i negativa konsekvenser för just verksamheten. Verksamhet kan syfta på en specifik tillgång eller på den verksamhet som påverkas av konsekvenser när oönskade händelser inträffar. Det är därmed otydligt vad begreppet *verksamhet* syftar på. När tillgångar ska identifieras är det av vikt att bestämma huruvida verksamhet ska anses vara en tillgång eller om en lägre abstraktionsnivå är nödvändig för att identifiera andra typer av tillgångar i den aktuella verksamheten.

Ett stöd i identifieringen av tillgångar är att avgränsa analysarbetet genom att välja utifrån vilket perspektiv tillgångar ska anses vara skyddsvärda. I Figur 1 ges exempel på hur olika perspektiv kan definieras för Försvarsmakten vid analys för ett planerat IT-system. Den innersta cirkeln anger att det är en tillgång som är skyddsvärd utifrån perspektivet IT-systemet. Nästa cirkel anger att tillgången är skyddsvärd från perspektivet av den verksamhet som det planerade IT-systemet ska stödja. Nästa cirkel anger att tillgången är skyddsvärd sett ur hela Försvarsmaktens perspektiv medan den yttre cirkeln anger att tillgången är skyddsvärd ur ett Sverige-perspektiv. Vilket perspektiv som väljs har därmed avgörande betydelse för utformningen av hotbeskrivningen och för avgränsandet av vilka tillgångar som ska beaktas.



Figur 1: Olika perspektiv för att identifiera tillgångar (Hallberg, Bengtsson och Karlzén, 2016).

2.2 Oönskad händelse

I sammanhanget säkerhetsanalys utgörs oönskade händelser av brott mot de säkerhetsegenskaper som är relevanta för den aktuella tillgången, exempelvis konfidentialitet, riktighet och tillgänglighet. Enligt H Säk Grunder (s. 47) är det väsentligt att oönskade händelser uttrycks tillräckligt specifikt för att möjliggöra de nödvändiga bedömningarna. För att förtydliga vad som sker med tillgången respektive hur detta sker föreslås att tillvägagångssättet bryts ut från den oönskade händelsen till ett eget informationselement (Hallberg, Bengtsson och Karlzén, 2016).

En oönskad händelse kan definieras som en negativ påverkan på en tillgång. Identifieringen av oönskade händelser underlättas därmed om det finns en fastställd uppsättning säkerhetsegenskaper som kan kategorisera de olika påverkanstyperna. På så vis utgörs identifieringen av oönskade händelser av att avgöra vilka säkerhetsegenskaper som är relevanta för var och en av tillgångarna. I Magerit 3.0 (Ministry of Finance and Public Administration, 2014) används konceptet dimensioner kopplat till tillgångar för att ge ett liknande stöd.

En ofta använd uppsättning med säkerhetsegenskaper för informationstillgångar är *konfidentialitet*, *riktighet* och *tillgänglighet*. Utgående från denna grundläggande uppsättning med säkerhetsegenskaper kan upp till tre oönskade händelser erhållas per tillgång där säkerhetsegenskaperna påverkas. Exemplet i Tabell 1 visar en oönskad händelse som påverkar tillgängligheten för tillgången

och där det har identifierats tre olika tillvägagångssätt som skulle kunna leda fram till att den oönskade händelsen realiseras. Ytterligare två oönskade händelser kan specificeras utifrån påverkan av konfidentialitet respektive riktighet, men dessa har inte tagits med i Tabell 1.

Det finns även förslag till utvidgningar av den grundläggande uppsättningen med säkerhetsegenskaper. Ett exempel är Parkerian hexad (Parker, 2012) där egenskaperna *nytta*, *autenticitet* och *innehav* (eng. *utility*, *authenticity* and *possession*) tillkommer, vilket skulle resultera i upp till sex oönskade händelser per tillgång. Det är därefter upp till säkerhetsanalysens genomförare att avgöra vilka av dessa potentiella oönskade händelser som är relevanta.

2.3 Konsekvensbeskrivning

De konsekvenser som oönskade händelser ger kan beskrivas och bedömas såväl kvalitativt som kvantitativt. Konsekvensbeskrivningen är den kvalitativa bedömningen av konsekvensen där det med ord, snarare än med enbart ett värde, beskrivs vilken negativ påverkan den oönskade händelsen får om den skulle inträffa. Att kvantitativt bedöma konsekvens enligt en given skala, för att få ett värde som underlättar jämförelse av olika risker, är en central del i bedömningen av risker. Konsekvensbeskrivningar syftar till att utgöra ett stöd i den kvantitativa bedömningen av konsekvensen samtidigt som de även kan ge spårbarhet och tydliggöra bakgrunden till de kvantitativa bedömningar som görs.

I H Säk Grunder beskrivs faktorer som påverkar omfattningen av konsekvenser. Dessa faktorer inkluderar tillgångens organisatoriska placering, hur kritisk den är för verksamheten och kostnaden för att återställa eller återskapa den. I Magerit 3.0 beskrivs liknande faktorer såsom återställandekostnad och otillgänglighetskostnad.

Det är av avgörande betydelse för utformningen av hotbeskrivningen att fastställa vilken omfattning av konsekvenser som ska beaktas. Omfattningen kan beskrivas som vilka perspektiv konsekvenserna ska beskrivas utifrån. Exempelvis kan det vid säkerhetsanalyser för planerade IT-system handla om IT-systemet, den verksamhet som nyttjar IT-systemet, organisationen där denna verksamhet bedrivs eller Sverige (Figur 1). Verksamhetsanalysen kan ge ett stöd i att välja vilket perspektiv som konsekvenserna ska beskrivas utifrån.

Att tillhandahålla ändamålsenliga konsekvensbeskrivningar kan kräva ett omfattande arbete. Om beskrivningarna är för generella kan de komma att sakna betydelse för bedömningen av konsekvensen. Vidare kan viss information vara så avgörande att den gör andra delar av konsekvensbeskrivningen överflödiga. Exempelvis leder hotbeskrivningar som inkluderar röjandet av hemlig information vid säkerhetsanalyser enligt H Säk Grunder till att konsekvensen är

given baserat på informationens klassning. Då blir det nödvändigt att avgöra om analys av eventuella ytterligare konsekvenser är meningsfullt.

2.4 Aktör

Aktören inkluderas som ett informationselement för att beskriva vem som ger upphov till att ett hot kan realiseras. Detta informationselement kan i standarder exempelvis kallas för hotkälla eller hotursprung, medan Försvarsmakten använder begreppet aktör. I H Säk Grunder finns ingen explicit definition av begreppet *aktör*, men ur resonemanget om aktörsdrivna hot går att utläsa att det med aktör avses *en individ, grupp, nätverk, organisation eller stat*. Denna beskrivning av en aktör stämmer väl överens med definitionen av aktör i Försvarsmaktens gemensamma riskhanteringsmodell (Försvarsmakten, 2009a) som använder definitionen *En enskild mänsklig individ, eller en sammanslutning av människor: en grupp, ett nätverk, en organisation, en stat, eller en sammanslutning av flera stater*.

Inom Försvarsmakten kategoriseras aktörer utifrån den säkerhetshotande verksamheten. De fem övergripande kategorierna som används är *främmande underrättelseverksamhet*, *kriminalitet*, *sabotage*, *subversion* och *terrorism*. Ett alternativt sätt att beskriva en aktör är att istället använda en kategorisering som beskriver vem aktören är. Ett exempel på sådan kategorisering föreslås i ett white paper från Intel (Casey, 2007) som beskriver ett antal standardmässiga kategorier för aktörer (Tabell 3). Att använda någon typ av kategorisering kan stödja arbetet med att identifiera relevanta aktörer.

Tabell 3: Kategorisering av aktörer enligt Casey (2007).

Intention	Aktör
Non-Hostile	Employee, Reckless
	Employee, Untrained
	Information Partner
Hostile	Anarchist
	Civil Activist
	Competitor
	Corrupt Government Official
	Cyber Vandal
	Data Miner
	Employee, Disgruntled
	Government Spy
	Government Cyberwarrior
	Internal Spy
	Irrational Individual
	Legal Adversary
	Mobster
	Radical Activist
	Sensationalist
	Terrorist
	Thief
	Vendor

Att enbart beskriva en aktör vid namn eller tillhörandes en viss kategori är inte tillräckligt underlag för att kunna bedöma risken. I H Säk Grunder föreslås att aktören dessutom beskrivs utifrån kapacitet, intention och tillfälle för varje hot. Detta förslag återges även i flera andra handböcker från Försvarsmakten (Försvarsmakten, 2006, 2009a, 2009b). Dessa tre perspektiv definieras enligt Tabell 4 och beskrivs utförligare i Försvarsmaktens Handbok bedömning

antagonistiska hot (Försvarsmakten, 2009b) där det även ges stöd i form av frågeställningar som kan nyttjas vid analysen.

Tabell 4: Definitioner för tillfälle, kapacitet och intention enligt (Försvarsmakten, 2009b).

Term	Definition
Tillfälle	En aktörs möjlighet i tid och rum att i direkt, indirekt eller överförd bemärkelse påverka en specifik skyddsvärd tillgång genom bruk av ett visst offensivt eller defensivt modus operandi[4].
Kapacitet	En aktörs resurser för att i direkt, indirekt eller överförd bemärkelse påverka en specifik skyddsvärd tillgång genom bruk av ett visst offensivt eller defensivt modus operandi.
Intention	En aktörs dolda, uttalade eller påvisade vilja att i direkt, indirekt eller överförd bemärkelse påverka en specifik skyddsvärd tillgång genom bruk av ett visst offensivt eller defensivt modus operandi.

Närbesläktat med Försvarsmaktens sätt att beskriva aktören föreslår Casey (2007) att aktören istället beskrivs utifrån de sju egenskaperna: Access, Outcome, Limits, Resources, Skills, Objective och Visibility. Dessa egenskaper sammanfaller med Försvarsmaktens indelning i tillfälle, kapacitet och intention, men erbjuder kompletterande perspektiv som ger möjlighet att tillföra mer detaljer till beskrivningen av aktörer.

2.5 Tillvägagångssätt

Ett tillvägagångssätt utgörs av en uppsättning med handlingar som en aktör kan nyttja för att realisera en oönskad händelse. Det kan finnas flera olika tillvägagångssätt som utlöser en oönskad händelse. Kunskap såväl om möjliga tillvägagångssätt som om sårbarheter dessa nyttjar är därmed central för bedömningen av sannolikheten för oönskade händelser. I H Säk Grunder används benämningarna modus operandi och metoder som begrepp motsvarande tillvägagångssätt. Ingen av benämningarna är framträdande i resonemangen kring bedömning av risker, men de omnämns i samband med bedömning av hotnivå och identifiering av sårbarheter.

Eftersom tillvägagångssätt utgör aktörens medel för att utnyttja sårbarheter kan beskrivningar av tillvägagångssätt stödja identifieringen av sårbarheter. Att

[4] Tillvägagångssätt

beskriva tillvägagångssätt kan därmed tjäna som ett verktyg under säkerhetsanalysen såväl som erbjuda spårbarhet avseende kopplingar mellan aktörer som sårbarheter. En inneboende svårighet återfinns i problemet med att beskriva tillvägagångssätt tillräckligt detaljerat för att det ska kunna bidra till analysen utan att arbetet att beskriva tillvägagångssättet eller dess bedömning blir alltför komplex.

Verktyg som kan nyttjas för att identifiera och beskriva tillvägagångssätt är attackträd (Schneier, 2000) och felanvändningsfall (Opdahl och Sindre, 2009).

2.6 Sårbarhet

Begreppet sårbarhet används som beteckning för brister i skyddet av en tillgång (Försvarsmakten, 2013). En sårbarhet är någonting som utnyttjas i ett tillvägagångssätt för att åstadkomma en oönskad händelse. Kunskap om sårbarheter är därmed nödvändig för bedömningen av sannolikheten för att ett hot realiseras.

Konceptet sårbarhet definieras i många dokument relaterade till bedömning av risker och definitionerna i de olika dokumenten är snarlika varandra. Alla definitionerna inkluderar exempelvis konceptet att sårbarheter kan utgöras av brister i skyddet av tillgångar. Vissa dokument inkluderar även andra allmänna beskrivningar av var sårbarheter kan återfinnas. Alberts och Dorofee (2001) klassificerar sårbarheter som organisatoriska eller tekniska. NIST (2012) beskriver, i kontexten riskanalyser för informationssystem, att sårbarheter även kan vara kopplade till den omgivande miljön. Att sårbarheter kan återfinnas utanför tillgångar och deras skydd gör det nödvändigt att, liksom vid identifiering av tillgångar, tydliggöra vilka perspektiv som ska beaktas. Vid säkerhetsanalyser för planerade IT-system är två exempel på möjliga perspektiv själva IT-systemet och den verksamhet som IT-systemet ska stödja (Figur 1).

2.7 Skyddsåtgärd

Skyddsåtgärderna utgör tillsammans det skydd som ska stoppa oönskade händelser mot tillgångarna från att realiseras. Vad gäller antagonistiska hot kan skyddsåtgärder exempelvis påverka aktörers intention genom att ha en avskräckande effekt eller genom att minska den illvilja som riktas mot organisationen. Skyddsåtgärderna kan också påverka vilken kapacitet och tillfälle som krävs för att hot ska kunna realiseras. Exempelvis kan en organisation öka sin kunskap om hoten genom säkerhetsanalyser, utbildningar eller övervakning.

Det finns svårigheter med att identifiera vilka skyddsåtgärder som är adekvata att använda för att förbättra skyddet. Det är även svårt att fastställa skyddsåtgärders kostnader eftersom de kan leda till omfattande indirekta kostnader. Exempelvis

kan en skyddsåtgärd ge upphov till en mängd falska positiva larm vilka är kostsamma att hantera. För att kunna avgöra om en tillkommande skyddsåtgärd är lämplig att införa krävs också kunskap om dess påverkan på relevanta risker. Vidare kan tillkommande säkerhetsåtgärder såväl tillföra nya sårbarheter som ge upphov till nya hot och påverka andra skyddsåtgärder, vilket kan försämra skyddet av aktuella tillgångar.

Förbättrade skyddsåtgärder kan medföra att användare känner sig tryggare med en högre exponering, vilket ökar aktörers tillfälle, och resulterar i en mindre minskning av risker än avsett. Denna aspekt av hur tillförandet av skyddsåtgärder påverkar exempelvis den acceptabla exponeringen illustreras av Adams (1999) med en risktermostat. Risktermostaten illustrerar hur minskad uppfattad risk kan leda till förändrat beteende för att öka den belöning som risktagandet ger.

I KSF (Försvarsmakten, 2014) regleras vilka grundläggande krav som ställs på skyddsåtgärder för Försvarsmaktens IT-system. Säkerhetsanalysen syftar till att identifiera tillkommande krav som kompletterar de som erhålls från KSF. Ett stöd för att identifiera olika typer av skyddsåtgärder är att klassificera dem utifrån någon egenskap, exempelvis utifrån när de genomförs som SIS föreslår. SIS delar in åtgärderna i kategorierna förebyggande, skadereducerande och återställande (SIS, 2015). Genom att klassificera skyddsåtgärder kan exempelvis avsaknad av vissa typer av skyddsåtgärder identifieras. Enbart förebyggande skyddsåtgärder kan exempelvis indikera brist på förmåga att hantera oönskade händelser när de väl inträffar.

3 Hotbeskrivningens utformning

Det kan tyckas som att den viktigaste delen vid analys av hot är genomförd när hoten har identifierats, men om inte hoten beskrivs på ett tydligt sätt i en hotbeskrivning kan de vara både svåra att förstå och bedöma i det fortsatta arbetet. Utöver vilka informationselement som ska ingå i en hotbeskrivning, vilket diskuteras i kapitel 2, kan det även vara av betydelse hur hotbeskrivningen utformas i skrift.

I kravhanteringsarbete är specificeringen av krav en egen del i arbetet som det läggs stor vikt på då det har visat sig att specificeringen av krav har tydlig inverkan på huruvida utvecklingsprojekt för IT-system lyckas. Under 1994 släpptes The CHAOS Report (The Standish Group International, 1994) som beskrev resultaten från en studie som bland annat fokuserade på att identifiera de vanligaste orsakerna till att projekt inom mjukvaruutveckling misslyckas. Med misslyckas avses att den levererade produkten inte motsvarar kraven, inte har levererats i tid eller till utsatt pris. *Brist på användardeltagande* var den vanligaste orsaken, men redan på andra plats återfanns *ofullständiga krav och specifikationer* följd av *förändrade krav och specifikationer* på tredje plats. Den vanligaste anledningen till att projekt avbryts innan arbetet är slutfört var *ofullständiga krav*. Samma studie identifierade även de vanligaste framgångsfaktorerna för projekt som bedömdes ha varit framgångsrika och då återfanns *tydligt specificerade krav* som den tredje vanligaste framgångsfaktorn.

Det finns två generella orsaker till att krav är felaktiga. Den första orsaken är att kraven har fel innehåll och därmed inte uttrycker det som var tänkt. Den andra orsaken är att kraven är specificerade på ett felaktigt sätt (Davis *m.fl.*, 1993). FOI genomförde under 2011 en studie på uppdrag från Försvarsmakten som resulterade i en ansats till hur krav ska formuleras för att de ska bli korrekt specificerade. Studien resulterade i en rapport (Hansson, Granlund och Hallberg, 2011) där åtta principer beskrevs som syftar till att omhänderta vanligt förekommande fel. Dessa principer har även legat till grund för det avsnitt i *Handbok Målsättningsarbete Tekniska system* (Försvarsmakten, 2015) som beskriver hur systemkrav ska formuleras.

Att formulera hot kan tänkas ha vissa paralleller med formulering av krav. I båda fallen är syftet med formuleringen att förmedla en beskrivning av något på ett så tydligt sätt som möjligt. För krav handlar det primärt om att beskriva vad systemet ska klara av på ett mätbart sätt som möjliggör verifiering av huruvida kravet är uppfyllt när det kravställda levereras, exempelvis ett IT-system. För hot handlar det om att beskriva en händelse som skulle kunna ha en negativ påverkan på verksamhetens tillgångar för att utifrån beskrivningen göra bedömningar av huruvida den resulterande risknivån kan accepteras eller om nya skyddsåtgärder behöver tillföras. Både för arbetet med krav och hot utgör formuleringen ett viktigt steg som lägger grunden för det fortsatta arbetet.

I avsnitten som följer görs en genomgång av de åtta principerna för kravformulering som har föreslogits av Hansson, Granlund och Hallberg (2011). De åtta principerna är: form, osammansatt, specificerat, entydigt, verifierbart, terminologi, lösningsoberoende och spårbarhet. Syftet med genomgången är att undersöka i vilken utsträckning principerna kan ge ett stöd även vid formulering av hotbeskrivningar.

3.1 Form

Inom kravformulering innebär principen *form* att alla krav uttrycks på samma form för att underlätta både granskning och omsättning till faktiska system. Genom att använda kravformuleringsmallar som stödjer den syntaktiska uppbyggnaden fås stöd i att få alla krav formulerade på samma form. Exempel på grundläggande mall är att kraven uttrycks på formen ”Systemet skall…”.

Principen för form är applicerbar även vid formulering av hot. Att uttrycka alla identifierade hot på samma form skulle kunna underlätta granskning av beskrivna hot, men även ge ett stöd i att säkerställa att all relevant information finns med i hotbeskrivningen. Principen för form kan exempelvis efterlevas genom att använda en mall som specificerar hur informationen ska struktureras när den uttrycks i skrift.

Under 2016 genomfördes en studie av hur strukturen för hotbeskrivningar påverkar samstämmigheten i bedömningen av hotens sannolikhet och konsekvens (Hallberg, Bengtsson och Karlzén, 2016). I studien jämfördes hotbeskrivningar strukturerade i form av löpande text med hotbeskrivningar i tabellform där de ingående informationselementen presenterades med namn och innehåll. Resultatet från studien tyder på att löpande text ger högre samstämmighet när icke-experter genomför bedömningar av sannolikhet och konsekvens. När experter bedömde sannolikhet och konsekvens var istället samstämmigheten högre när hotbeskrivningen strukturerades i tabellform. Vilken struktur som är bäst att använda vid formulering av hot beror således på målgruppen för hotbeskrivningarna.

3.2 Osammansatt

Inom kravformulering innebär principen *osammansatt* att flera krav inte ska uttryckas i samma kravformulering. Varje krav ska uttrycka ett och endast ett krav. Sammansatta krav kan ofta identifieras genom att kravet innehåller *och* alternativt *eller*. Uppräkningar genom punktlistor eller numrerade listor är också kännetecken på ett sammansatt krav.

Syftet med att eftersträva osammansatta krav är att underlätta verifieringen av kravets uppfyllnad då det uttrycker ett och endast ett krav. Hotbeskrivningar

används istället som underlag för att bedöma sannolikhet och konsekvens och huruvida beskrivningen är sammansatt påverkar då istället dessa två bedömningar. Att en hotbeskrivning är sammansatt innebär att flera olika hot uttrycks i en och samma beskrivning. För sannolikheten bedöms då hur troligt det är att den beskrivna kombinationen av hot inträffar. På samma sätt återspeglar bedömningen av konsekvens den konsekvens som uppstår om motsvarande kombination av hot skulle realiseras.

För hotbeskrivningar är det inte säkert att det alltid är eftersträvansvärt att alla hotbeskrivningar ska vara osammansatta eftersom de inte används till verifiering. Det viktigaste är att vara medveten om huruvida det faktiskt är flera hot sammansatta till ett som bedöms samt vad bedömningen av sannolikhet faktiskt avser. Exempel på sammansatt del i en hotbeskrivning återfinns i H Säk Grunder (sida 51) där den oönskade händelsen specificeras enligt följande.

”Inbrott i datalektionssal och omfattande förstöring eller stöld av datorutrustning”

I exemplet är datorutrustning angiven som tillgång och den oönskade händelsen omfattar både förstöring av datorutrustning och stöld av datorutrustning. Då det är själva datorutrustningen som har angetts som tillgång, inte någon information på datorerna, blir konsekvensen att ny datorutrustning behöver inhandlas oavsett om utrustningen förstörs eller stjäls. Det kan då vara rimligt att ha en hotbeskrivning som inte uppfyller principen om osammansatta beskrivningar.

Om det istället hade varit informationen på datorutrustningen som varit angiven som tillgång kan konsekvensen tänkas vara olika om datorutrustningen skulle förstöras eller stjälas. En sammansatt hotbeskrivning skulle då kunna göra det otydligt för vad sannolikheten och konsekvensen egentligen ska bedömas.

3.3 Specificerat

Inom kravformulering innebär principen *specificerat* att krav ska formuleras kort och koncist, men med tillräcklig information. Krav ska enbart innehålla den mängd information som gör att det är fullständigt och inte kan feltolkas. Krav som är ofullständiga och inte innehåller tillräcklig information kan komma att missförstås. Dessutom kan krav som innehåller överflödig information medföra att den väsentliga informationen döljs.

Principen är direkt överförbar på formuleringen av hot. Ett sätt att stödja uppfyllandet av principen är att tydligt beskriva vilka delar som ska ingå i hotbeskrivningar, vilket beskrivs i kapitel 2.

3.4 Entydigt

Inom kravformulering innebär principen *entydigt* att ord som kan ha många olika betydelser ska undvikas då dessa gör det svårare att verifiera att krav är uppfyllda. Undvik även vaga ord såsom *stor*, *bra*, *snabb* eller *effektiv* då dessa inte heller går att verifiera. Istället ska riktiga värden användas, som exempelvis *7* som går att verifiera. Ytterligare exempel på vaga ord är *stödja, medge, ge förutsättningar, erbjuda* och *försvåra*.

På samma sätt som för kravformulering är det eftersträvansvärt att formulera hot utan att använda vaga ord med oklar betydelse, exempelvis *dyrbar*, *dålig* eller *svag*. Användandet av vaga ord ökar tolkningsutrymmet för vad det beskrivna hotet innebär, vilket kan påverka bedömningen av både sannolikheten och konsekvensen. Det är inte alltid möjligt att helt undvika att använda ord med oklar betydelse, men med en terminologilista kan negativa effekter minskas. I terminologilistan beskrivs den avsedda innebörden av de vaga ord som ändå har använts i hotbeskrivningarna. Exempel på hur innebörden av vaga ord kan beskrivas i en terminologilista återges i Tabell 5.

Tabell 5: Exempel på terminologilista för vaga ord.

Term	**Avsedd innebörd**
Dyrbar tillgång	Tillgången har ett monetärt värde som överstiger 10% av organisationens omsättning.
Svag signal	Signalstyrkan är inte tillräckligt hög för att kunna upprätthålla kommunikationen utan att riskera avbrott.

3.5 Verifierbart

Inom kravformulering innebär principen *verifierbart* att varje krav ska vara verifierbart för att göra det möjligt att avgöra om det system som har tagits fram uppfyller de ställda kraven. Ett sätt att göra det möjligt att avgöra huruvida ett krav är uppfyllt är att det anges med mätbara värden, exempelvis ”Systemet skall kunna vara operativt i 8 timmar genom batteridrift”.

Principen för verifierbart är inte direkt applicerbar på hotbeskrivningar som helhet eftersom dessa används som underlag för att bedöma sannolikhet och konsekvens. Däremot kan principen vara applicerbar på delar av den information som kan tänkas behöva vara inkluderad i en hotbeskrivning. Ett exempel är

beskrivningen av befintliga sårbarheter där det skulle kunna krävas att existensen av nämnda sårbarheter verifieras.

3.6 Terminologi

Inom kravformulering innebär principen *terminologi* att en lista med begrepp och förklaringar ska upprättas för de använda begrepp som kan tolkas på olika sätt. De begrepp som behöver förklaras ska vara definierade och tillgängliga under kravhanteringen för att krav ska kunna anses vara fullständiga.

Principen för terminologi är applicerbar på hot på samma sätt som på krav. I båda fallen är det eftersträvansvärt att beskrivningarna inte innehåller begrepp eller akronymer som inte är definierade. För att undvika tvetydigheter sammanställs definitionerna av dessa begrepp och akronymer i en terminologilista som behöver finnas tillgänglig tillsammans med hotbeskrivningarna. Exempel på hur begrepp kan definieras i en terminologilista återges i Tabell 6.

Tabell 6: Exempel på terminologilista för begrepp och akronymer.

Term	Definition	Källa
Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten	SIS HB 550 Utgåva 3
Risk	Kombination av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad	SIS HB 550 Utgåva 3
Riskhanteringsåtgärd	Åtgärd för att bibehålla och/eller förändra risker	SS-ISO 31000:2018

3.7 Lösningsoberoende

Inom kravformulering innebär principen *lösningsoberoende* att krav i största möjliga mån ska uttryckas lösningsoberoende. Krav ska formuleras för att uttrycka vad ett system ska klara av, inte hur kravet ska realiseras. När krav innehåller specifika lösningar minskar utrymmet vid realisering av systemet, vilket kan leda till att bättre och billigare lösningar avgränsas bort.

Principen för lösningsoberoende är inte applicerbar vid formulering av hot då det inte nödvändigtvis är som så att beskrivandet av specifika lösningar är något negativt. Vad som utgör en lösning i kontexten hotbeskrivningar varierar med vilket informationselement som beaktas. Avseende en skyddsåtgärd kan en

detaljerad beskrivning av en specifik lösning vara ett bättre underlag för bedömning av sannolikhet än en mer övergripande beskrivning. Exempelvis att beskriva att Färist 4.0 ska användas med en specificerad konfiguration istället för att enbart beskriva skyddsåtgärden som brandvägg. Däremot minskas det möjliga lösningsutrymmet för den som ska införa skyddsåtgärden, vilket kan leda till lösningar som inte är optimala ur ett verksamhetsperspektiv, exempelvis avseende kostnad.

En hotbeskrivning som exempelvis innehåller en väldigt detaljerad beskrivning av tillvägagångssättet kan underlätta när sannolikhet och konsekvens ska bedömas. Samtidigt kan antalet hot snabbt bli stort om varje möjligt tillvägagångssätt ska specificeras separat i ett eget hot. Ett exempel kan vara ett tillvägagångssätt som beskrivs som *inbrott genom forcering av byggnadens västra ytterdörr med hjälp av kofot* jämfört med att enbart beskriva tillvägagångssättet som *inbrott*. Vilken detaljnivå som ska eftersträvas i hotbeskrivningar blir en avvägning mellan vilken detaljnivå som är nödvändig för att kunna göra bedömningarna och hur många hot som det är praktiskt möjligt att hantera i analysarbetet.

3.8 Spårbart

Inom kravformulering innebär principen *spårbart* att krav ska kunna spåras tillbaka till sina respektive källor i form av exempelvis bakomliggande förmåga, dokument eller händelse. Varje krav förses med en unik identifierare för att möjliggöra att funktioner och egenskaper i design och realisering kan spåras tillbaka till de krav de är avsedda att tillgodose.

Principen för spårbarhet är även applicerbar för hotbeskrivningar. Vid formulering av hot är det nödvändigt med en unik identifierare som kan användas för att referera till varje identifierat hot. Det är dessutom nödvändigt att ha en spårbarhet tillbaka till hotets ursprung för att exempelvis underlätta regelbunden uppdatering av säkerhetsanalyser.

4 Förslag på innehåll och utformning

I detta kapitel presenteras ett förslag på vilka informationselement som bör ingå i en hotbeskrivning samt vilka principer som bör följas vid dess utformning. Förslaget utgår från de informationselement som identifierades i kapitel 2 samt de principer som diskuterades i kapitel 3. Syftet med detta förslag är inte att det ska vara en slutlig version utan snarare en utgångspunkt för vidare diskussion och utveckling av kunskapen om vilken information som behöver ingå i en hotbeskrivning och hur den ska utformas.

Den grundläggande tanken med att dela upp hotbeskrivningar i informationselement är att förtydliga vad som ska ingå i en hotbeskrivning samt att underlätta identifiering och specificering av dessa ingående element. Med väl specificerade hotbeskrivningar ges förutsättningar att kunna bedöma sannolikhet och konsekvens. De informationselement som diskuterades i kapitel 2 och som föreslås utgöra innehållet i en hotbeskrivning beskrivs kortfattat i Tabell 7. De föreslagna informationselementen relaterar till varandra enligt följande beskrivning.

Aktörer använder tillvägagångssätt för att utnyttja sårbarheter vilket, trots existerande skyddsåtgärder, kan realisera en oönskad händelse som påverkar informationssäkerhetsegenskaper hos tillgångar och resulterar i konsekvenser.

Tabell 7: Föreslagna informationselement

Informations-element	**Beskrivning**
Tillgång	En tillgång är något som bedöms vara kritiskt eller på annat sätt ha ett särskilt värde för den verksamhet som analyseras. Tillgångar utgör utgångspunkten för genomförandet av en säkerhetsanalys.
Oönskad händelse	En oönskad händelse är något som medför en negativ påverkan på en tillgång. I kontexten säkerhetsanalys innebär en oönskad händelse en påverkan av säkerhetsegenskaper för en tillgång. Givet en tillgång och en uppsättning av säkerhetsegenskaper identifieras oönskade händelser genom att avgöra vilka kombinationer av tillgången och säkerhetsegenskaperna som är relevanta. En grundläggande uppsättning med säkerhetsegenskaper för informationstillgångar är konfidentialitet, riktighet och tillgänglighet.
Konsekvens-beskrivning	En konsekvensbeskrivning innehåller kvalitativa bedömningar av den negativa påverkan som en oönskad händelse medför, där konsekvensen beskrivs med ord, snarare än med enbart ett värde. Konsekvensbeskrivningen utgör underlag för den kvantitativa bedömningen av konsekvensen, ger spårbarhet och tydliggör bakgrunden till den kvantitativa bedömningen.
Aktör	En aktör är den part som genom ett tillvägagångssätt ligger bakom realiserandet av en oönskad händelse. Med aktör kan avses exempelvis en individ, grupp, organisation eller stat. Egenskaper som beskriver en aktör, exempelvis kapacitet, intention och tillfälle, har stor betydelse för sannolikheten för att ett hot realiseras.
Tillvägagångssätt	Tillvägagångssätt beskriver en aktörs förfarande som leder till att en oönskad händelse inträffar. Kunskap om möjliga tillvägagångssätt är nödvändigt för bedömningen av sannolikheten för att ett hot realiseras.

Informations-element	Beskrivning
Sårbarheter	Sårbarheter utgörs huvudsakligen av brister i skyddet av tillgångar. Sårbarheter kan klassificeras som organisatoriska eller tekniska. En sårbarhet är någonting som utnyttjas av en aktör i ett tillvägagångssätt för att realisera ett hot. Kunskap om sårbarheter är nödvändigt för bedömningen av sannolikheten för att ett hot realiseras.
Skyddsåtgärder	En skyddsåtgärd är något som syftar till att minska sannolikheten att ett hot realiseras genom att antingen minska sårbarheten eller påverka en aktör. Den samlade mängden skyddsåtgärder utgör skyddet av den verksamhet som analyseras. Skyddsåtgärder kan klassificeras utifrån olika egenskaper, exempelvis baserat på om de syftar till att påverka aktörers intention, kapacitet eller tillfälle alternativt baserat på när skyddsåtgärden genomförs såsom förebyggande, skadereducerande eller återställande.

Med utformning avses hur de föreslagna informationselementen i skrift formuleras till en komplett hotbeskrivning. En delmängd av de principer för kravformulering som diskuterades i kapitel 3 bedömdes även ha bäring vid formulering av hotbeskrivningar. Principerna entydighet och terminologi för kravformulering har för hotbeskrivningar kombinerats i principen entydighet. Följande principer föreslås vid formulering av hotbeskrivningar.

- **Form**
  Uttryck alla hotbeskrivningar på samma form.
- **Osammansatt**
  Undvik att formulera flera hot i samma hotbeskrivning om de resulterar i olika konsekvenser.
- **Specificerad**
  Formulera hotbeskrivningen så att den enbart innehåller den information som är nödvändig.
- **Entydig**
  Undvik att använda vaga ord som ökar hotbeskrivningens tolkningsutrymme samt definiera alla begrepp och akronymer som används i hotbeskrivningen

- **Spårbar**
  Tilldela varje hotbeskrivning en unik identifierare samt referera tillbaka till respektive hots ursprungskälla.

5 Studie av hotbeskrivningars påverkan på bedömningar

För att bidra till kunskapen om hur innehållet i hotbeskrivningar påverkar bedömningen av risker genomfördes en kvantitativ enkätstudie utgående från de föreslagna informationselementen. Den grundläggande idén bakom studien var att ställa upp ett antal hypoteser om hur bedömningen av sannolikhet och konsekvens för ett hot påverkas av hotbeskrivningens innehåll samt bedömarens erfarenhet. Utgående från insamlande data används statistiska metoder för att dra generella slutsatser. Som grund för genomförandet av studien formulerades hypoteser utgående från frågeställningar kopplade till hotbeskrivningars påverkan på bedömning av risker. För att samla in data nyttjades enkäter med hotbeskrivningar utgående från vilka respondenterna fick bedöma sannolikhet och konsekvens för hoten. Respondenterna fick via enkäterna också genomföra en självskattning av sin expertis inom området, kunskapsnivå etc. När data hade samlats in testades de formulerade hypoteserna med hjälp av statistiska metoder.

För att begränsa studiens omfattning valdes informationselementet aktör ut som den del av hotbeskrivningen som främst skulle studeras. Enligt H Säk Grunder (Försvarsmakten, 2013) ska konsekvensen bedömas innan aktören specificeras. Det finns fördelar med detta förfarande, exempelvis att antalet konsekvensbedömningar minskas. Andra metoder för riskbedömning, exempelvis Försvarsmaktens gemensamma riskahanteringsmodell (Försvarsmakten, 2009a), specificerar dock att konsekvensen bedöms i samma steg som sannolikheten, dvs. med hela hotbeskrivningen som underlag. Leder denna skillnad avseende i vilket skede av analysen som konsekvensen bedöms till skillnader avseende bedömningen av konsekvensen av att hot realiseras? För att analysera denna frågeställning formulerades hypotesen:

1) *Bedömningen av konsekvens påverkas av specificerad aktör.*

En möjlig omständighet är att respondenter som inte är säkra på sina bedömningar lägger större betydelse vid specificeringen av aktör när konsekvensen ska bedömas, medan de respondenter som är säkra på sina bedömningar inte lägger någon betydelse vid specificeringen av aktör när konsekvensen ska bedömas. För att analysera detta formulerades hypoteserna:

2) *För respondenter som inte är säkra på sina bedömningar påverkas bedömningen av konsekvens av specificerad aktör.*

3) *För respondenter som är säkra på sina bedömningar påverkas bedömningen av konsekvens av specificerad aktör.*

En specifik aktör som kan tänkas påverka bedömningen av konsekvens är främmande makt. En möjlighet är att påverkan av främmande makt som

specificerad aktör inte gäller för de som är vana vid att genomföra säkerhetsanalyser. För att analysera detta formulerades hypoteserna:

4) *När aktören specificeras som främmande makt bedöms konsekvensen som högre.*

5) *När aktören specificeras som främmande makt bedömer respondenter som är vana vid att genomföra säkerhetsanalyser konsekvensen som högre.*

När det inte finns någon kunskap om vilka svar som är korrekta kan istället samstämmigheten mellan respondenternas svar analyseras (Shanteau, 2015). Om samstämmigheten mellan respondenterna är för låg bör inte deras svar användas som underlag för beslut, dvs. de erhållna svaren ger sammantaget inte någon bild av vad det korrekta svaret är. Oavsett om specificering av aktör påverkar de genomsnittliga bedömningarna av konsekvens eller ej, kan den påverka samstämmigheten mellan respondenternas bedömningar. För att analysera denna frågeställning formulerades hypotesen:

6) *Samstämmigheten mellan respondenternas bedömningar av konsekvens är högre när aktören är specificerad än när aktören är ospecificerad.*

Samstämmigheten mellan respondenternas bedömning av konsekvens kan påverkas av att respondenterna har olika grad av expertis inom området. Är respondenter med hög expertis mer samstämmiga i sina bedömningar av konsekvens än respondenter med låg expertis? För att analysera denna frågeställning formulerades hypoteserna:

7) *Samstämmigheten mellan respondenternas bedömningar av konsekvens är högre för respondenter med hög expertis än för respondenter med låg expertis.*

8) *Samstämmigheten mellan respondenternas bedömningar av konsekvens är högre för de respondenter som är säkra på sina bedömningar än för de respondenter som är osäkra på sina bedömningar.*

Om tillgången är informationsklassificerad finns det en koppling till konsekvensskalan som anges i H Säk Grunder. Därmed borde samstämmigheten mellan respondenterna vara högre för hotbeskrivningar som anger resultatet av en informationsklassificering för tillgången. För att analysera denna frågeställning formulerades hypotesen:

9) *Samstämmigheten mellan respondenternas bedömningar av konsekvens är högre när hotbeskrivningen inkluderar resultatet av en informationsklassificering för tillgången.*

Hypoteser motsvarande hypoteserna 1–9 formulerades även för bedömningar av sannolikhet:

10) *Bedömningen av sannolikhet påverkas av specificerad aktör.*
11) *För respondenter som inte är säkra på sina bedömningar påverkas bedömningen av sannolikhet av specificerad aktör.*
12) *För respondenter som är säkra på sina bedömningar påverkas bedömningen av sannolikhet av specificerad aktör.*
13) *När aktören specificeras som främmande makt bedöms sannolikheten som högre.*
14) *När aktören specificeras som främmande makt bedömer respondenter som är vana vid att genomföra säkerhetsanalyser sannolikheten som högre.*
15) *Samstämmigheten mellan respondenternas bedömningar av sannolikhet är högre när aktören är specificerad än när aktören är ospecificerad.*
16) *Samstämmigheten mellan respondenternas bedömningar av sannolikhet är högre för respondenter med hög expertis än för respondenter med låg expertis.*
17) *Samstämmigheten mellan respondenternas bedömningar av sannolikhet är högre för de respondenter som är säkra på sina bedömningar än för de respondenter som är osäkra på sina bedömningar.*
18) *Samstämmigheten mellan respondenternas bedömningar av sannolikhet är högre när hotbeskrivningen inkluderar resultatet av en informationsklassificering för tillgången.*

Tidigare arbeten indikerar att samstämmigheten mellan respondenter är lägre vid bedömning av sannolikhet än vid bedömning av konsekvens (Hallberg, Bengtsson och Karlzén, 2016; Hallberg *m.fl.*, 2017), vilket antyder att det är svårare att bedöma sannolikhet än konsekvens. För att analysera denna frågeställning formulerades hypotesen:

19) *Samstämmigheten är högre vid bedömningar av konsekvens än vid bedömningar av sannolikhet.*

Ytterligare en frågeställning kopplad till bedömningar av sannolikhet och konsekvens gäller huruvida dessa bedömningar påverkar varandra. En möjlighet är att bedömare undviker kombinationerna hög sannolikhet och hög konsekvens respektive låg sannolikhet och låg konsekvens. För att analysera denna frågeställning formulerades hypotesen:

20) Korrelationen mellan bedömningarna av sannolikhet och konsekvens är negativ.

Givet den struktur för hotbeskrivningar som ges av informationselementen kan de beskrivningar som används för att specificera de olika delarna i denna struktur användas för att skapa regressionsmodeller vilka syftar till att estimera respondenternas bedömningar av sannolikhet och konsekvens. Utifrån de erhållna modellerna är det möjligt att dra slutsatser om de delar av hotbeskrivningarna som modellerna indikerar har betydelse för skattningen av respondenternas bedömningar.

I återstoden av detta kapitel presenteras hur studien genomfördes och analyserades. I avsnitt 5.1 presenteras framtagandet av enkäter för att samla in data som kan användas för att testa de formulerade hypoteserna. I avsnitt 5.2 beskrivs insamlandet av data med hjälp av enkäterna. I avsnitt 5.3 redogörs för analysen av insamlade data.

5.1 Framtagandet av enkäter

Det första steget i framtagandet av enkäterna var att skapa ett scenario. Att ha ett scenario underlättar framtagandet av konkreta hot som respondenterna ska bedöma. Samtidigt ger ett scenario även en kontext för respondenterna att utgå ifrån när hoten ska bedömas. Det scenario som togs fram beskrev en fiktiv organisation med ett flertal kontor runtom i Sverige. Den fiktiva organisationen hanterar i viss utsträckning information som omfattas av sekretess i sin verksamhet.

I syfte att underlätta framtagandet av hotbeskrivningar som lämpar sig för att testa uppställda hypoteser användes ett Excel-ark där hotbeskrivningarna delades upp i de informationselement som föreslogs i kapitel 4. Dessa informationselement sågs som möjliga informationselement och det är därmed inte nödvändigt att varje framtagen hotbeskrivning innehåller dem alla.

Framtagandet av hotbeskrivningar till enkäterna gjordes genom en kombination av mindre workshops med 2–4 deltagare och enskilt arbete däremellan. När en första version av hotbeskrivningarna var framtagen testades de först på två andra forskare inom området för att få återkoppling i form av förbättringsförslag.

Framtagandet av enkäterna utgick från att respondenterna ska vara anonyma. För att ändå kunna säga något om gruppen av respondenter så formulerades ett antal frågor om respondenternas arbetsuppgifter. Frågorna var så kallade självskattningsfrågor där respondenterna själva skulle bedöma hur väl olika påståenden stämmer överens med deras arbetsuppgifter och kunskapsnivå. Syftet med frågorna var att identifiera i vilken utsträckning respondenterna bedömer risker i sitt arbete och låg till grund för att kunna skapa grupperingar av respondenter som själva uppfattar sig ha liknande förutsättningar.

Den genomförda studiens hypoteser relaterar i hög grad till hur aktören specificeras i hotbeskrivningen. För att stödja testningen av hypoteserna togs två olika enkäter fram. De två enkäterna var identiska förutom att aktören specificerades olika i nio av de tio hotbeskrivningarna. I fortsättningen används benämningarna enkät A och enkät B för de två enkäterna.

Slutligen genomfördes ett test av enkät A och enkät B genom att fem personer med goda kunskaper inom området fick prova att fylla i en enkät. Personerna fick i uppgift att gå igenom varje hotbeskrivning för att identifiera eventuella felaktigheter eller olyckliga formuleringar som skulle kunna missförstås. Efter testet beaktades ändringsförslagen och en ny version av enkät A respektive enkät B skapades.

5.2 Insamling av enkätsvar

Den första insamlingen av enkätsvar genomfördes under en heldag då ett flertal möjliga respondenter fanns samlade på samma plats. Tillfället sågs som lämpligt för genomförandet av datainsamling då de möjliga respondenterna bedömdes i stor utsträckning arbeta med frågor som relaterar till olika typer av riskbedömningar.

Under inledningen av insamlingstillfället gavs en kort presentation av den fiktiva organisation som utgjorde scenariot som respondenterna skulle utgå från när de bedömde de hot som beskrevs i enkäten. Därefter hade respondenterna drygt femton minuter på sig att besvara enkäterna. De enkäter som delades ut till respondenterna var sorterade så att varannan var enkät A och varannan var enkät B. På så sätt var det möjligt att få ett liknande antal enkätsvar för de två enkäterna. Totalt återlämnades 65 komplett ifyllda enkäter, fördelat på 32 av enkät A och 33 av enkät B.

Insamlingstillfälle två till och med fem skedde i samband med genomförande av FOI:s kurser inom IT-säkerhet. Kursdeltagarna bedömdes arbeta med IT-säkerhetsrelaterade frågor, dock med en varierande förkunskap om genomförandet av säkerhetsanalyser. Kursdeltagarna fick möjlighet att besvara fylla i en av enkäterna under lediga stunder. Då det inte fanns möjlighet till muntlig presentation av den fiktiva organisationen som utgjorde scenariot fick deltagarna istället en motsvarande skriftlig beskrivning. Även vid dessa insamlingstillfällen var enkäterna sorterade så att varannan var enkät A och varannan var enkät B. Utfallet från de fem insamlingstillfällena redovisas i Tabell 8.

Tabell 8: Utfall för varje insamlingstillfälle.

Tillfälle	Enkät A	Enkät B	Totalt
1	32	33	65
2	5	5	10
3	8	9	16
4	8	9	17
5	9	3	10

5.3 Analys av data från enkäterna

Analysen av insamlade data utgick från de hypoteser som presenterades i inledningen av kapitel 5. För att testa hypoteserna användes följande angreppssätt.

- T-test används för att avgöra om det finns signifikanta skillnader mellan medelvärden för olika grupper (Warner, 2013).
- Krippendorff's alpha (KA) (Krippendorff, 2011) används för beräkning av samstämmighet avseende respondenternas bedömningar av sannolikhet och konsekvens.
- Regressionsmodeller används för att avgöra de olika informationsdelarnas betydelse för bedömningar av sannolikhet och konsekvens (Warner, 2013).

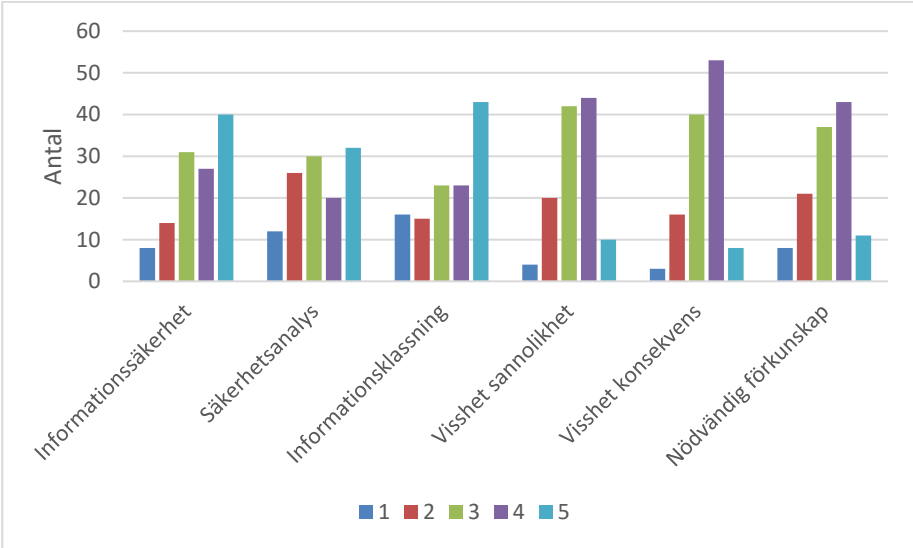
Den statistiska analysen genomfördes i SPSS version 25 och beräkningen av KA-värden genomfördes med SPSS-makrot KALPHA (Hayes och Krippendorff, 2007). KALPHA tillhandahåller förutom själva KA-värdena även 95 procentiga konfidensintervall (95% KI) för dessa värden. Utgående från dessa konfidensintervall är det möjligt att avgöra om det finns en statistiskt signifikant skillnad mellan två KA-värden. Med statistisk signifikans avses, om inte något annat anges, p-värden under 0,05 ($p < 0,05$). Med konfidensintervall (KI) avses i den fortsatta texten 95-procentiga konfidensintervall. Med specificerade KI finns det en statistiskt signifikant skillnad mellan motsvarande värden ifall deras respektive KI inte överlappar. Även om två KI överlappar kan det dock finnas en signifikant skillnad mellan motsvarande värden. För att avgöra om det finns en

statistiskt signifikant skillnad mellan två värden med överlappande KI krävs beräkningar utgående från dessa värden och deras respektive KI[5].

Av vikt för analysen är att det inte blev någon form av snedfördelning avseende vana att arbeta med informationssäkerhet, säkerhetsanalyser och informationsklassning samt förkunskap mellan de två grupper av respondenter som besvarade enkät A respektive enkät B. För att undersöka detta analyserades svaren på de i enkäterna inkluderade frågorna gällande arbetsuppgifter, visshet avseende bedömningar och förkunskap. Genomförda tester visar att det inte finns några statistiskt signifikanta skillnader avseende medelvärdena för svaren på dessa frågor mellan de som besvarade enkät A respektive enkät B. Fördelningen av svaren på frågorna återfinns i Figur 2.

Förhållandet (korrelationerna) mellan svaren återfinns i Tabell 9. Alla korrelationerna är positiva och signifikanta, dvs. högre svar på en fråga hänger ihop med högre svar på de andra frågorna. De starkaste korrelationerna, mellan svaren gällande arbetsuppgifter respektive svaren gällande visshet avseende bedömningar och förkunskap, är de kopplade till genomförandet av säkerhetsanalyser.

[5] En förklaring av skillnaden mellan två värdens överlappande konfidensintervall och signifikant skillnad mellan dessa värden finns exempelvis via http://www.cscu.cornell.edu/news/statnews/Stnews73insert.pdf.



Figur 2: Fördelningen av de 120 respondenternas svar på de tre frågorna gällande arbetsuppgifter (*Informationssäkerhet*, *Säkerhetsanalys* och *Informationsklassning*), de två frågorna gällande visshet avseende bedömningar (*Visshet sannolikhet* och *Visshet konsekvens*) samt frågan gällande huruvida respondenten hade nödvändig förkunskap (*Nödvändig förkunskap*). Staplarna representerar hur många respondenter som valde respektive alternativ för de sex frågorna, dvs. svarsalternativ 1 (med betydelsen *Instämmer inte alls* eller *Aldrig* beroende på fråga) till 5 (med betydelsen *Instämmer helt* eller *Flera gånger per år* beroende på fråga).

För att kunna kontrollera att de två grupperna som svarade på enkät A respektive enkät B inte skiljer sig åt med avseende på genomsnittet av gruppens bedömning av sannolikhet och konsekvens för ett specifikt hot, var en av hotbeskrivningarna identisk på de två enkäterna. Genomförda tester visar att det inte finns någon statistiskt signifikant skillnad avseende bedömningen av sannolikhet respektive konsekvens mellan de som bedömde detta hot på enkät A respektive enkät B.

Tabell 9: Korrelationer mellan svaren på frågorna gällande arbetsuppgifter, visshet avseende bedömningar och förkunskap. Frågorna avseende arbetsuppgifter gällde informationssäkerhet (IS), Säkerhetsanalys (SA) och informationsklassning (IK). Frågorna avseende visshet avseende bedömningarna gällde sannolikhet (VS) och konsekvens (VK). Frågorna avseende förkunskap gällde huruvida respondenten ansåg sig ha nödvändig förkunskap för att genomföra bedömningarna (FK).

	IS	SA	IK	VS	VK	FK
IS	1	0,558**	0,570**	0,289*	0,249*	0,371**
SA	0,558**	1	0,575**	0,366**	0,365**	0,434**
IK	0,570**	0,575**	1	0,335**	0,289*	0,398**
VS	0,289*	0,366**	0,335**	1	0,826**	0,750**
VK	0,249*	0,365**	0,289*	0,826**	1	0,730**
FK	0,371**	0,434**	0,398**	0,750**	0,730**	1

* $p < 0,01$; ** $p < 0,001$

5.3.1 Test av hypoteser relaterade till bedömningen av konsekvens

I detta avsnitt testas de hypoteser som relaterar till respondenternas bedömning av konsekvens. För att testa hypotes 1, 2 och 3 jämförs erhållna medelvärden för de hotbeskrivningar där specificeringen av aktör skiljer sig mellan enkät A och enkät B. Denna skillnad finns mellan nio av de tio hotbeskrivningarna i enkäterna.

1) *Bedömningen av konsekvens påverkas av specificerad aktör.*

Det finns inget generellt stöd för hypotesen då genomförda tester enbart visar på signifikanta skillnader i konsekvensbedömningen för två av de nio hotbeskrivningarna. I de två versionerna av den första hotbeskrivningen med signifikanta skillnader specificeras aktören som aktivister respektive kriminella. I de två versionerna av den andra hotbeskrivningen med signifikanta skillnader specificeras aktören som främmande makt respektive inte alls.

2) *För respondenter som inte är säkra på sina bedömningar påverkas bedömningen av konsekvens av specificerad aktör.*

För de respondenter som inte är säkra på sina bedömningar av konsekvens finns inga signifikanta skillnader mellan de två versionerna för något av hoten. Därmed finns det inget generellt stöd för hypotesen. Med respondenter som inte är säkra på sina bedömningar avses de som svarade 1 eller 2 på den femgradiga skalan tillhörande frågan gällande visshet avseende bedömningarna av

konsekvens, vilket var utfallet för 34 respektive 25 respondenter för enkät A respektive enkät B.

3) *För respondenter som är säkra på sina bedömningar påverkas bedömningen av konsekvens av specificerad aktör.*

För de respondenter som är säkra på sina bedömningar av konsekvens finns inga signifikanta skillnader mellan de två versionerna för något av hoten. Därmed finns det inget generellt stöd för hypotesen. Med respondenter som är säkra på sina bedömningar avses de som svarade 4 eller 5 på den femgradiga skalan tillhörande frågan gällande visshet avseende bedömningarna av konsekvens, vilket var utfallet 27 respektive 34 respondenter för enkät A respektive enkät B.

Resultaten avseende de tre första hypoteserna visar på att det finns spår av att specifikationen av aktör kan påverka bedömningen av konsekvens. För majoriteten av de nio hotbeskrivningar, där denna skillnad i specifikationen av aktör återfinns, finns det dock ingen statistiskt signifikant skillnad. Det finns dessutom inga statistiskt signifikanta skillnader alls för de två grupper med respondenter som inte är säkra respektive är säkra på sina bedömningar. Därmed finns det inget generellt stöd för hypotesen.

4) *När aktören specificeras som främmande makt bedöms konsekvensen som högre.*

Istället för att titta på de specificerade hoten parvis, där den enda skillnaden utgörs av specificeringen av aktör, kan resultaten för alla de hotbeskrivningar där aktören är specificerad som främmande makt läggas samman och jämföras med alla resultaten för motsvarande hotbeskrivning med annan specificering av aktör. Genom att lägga samman resultaten för flera hotbeskrivningar blir antalet datapunkter större, vilket är fördelaktigt när signifikansen hos skillnaden mellan olika värden testas. De genomförda testerna visar att bedömningarna av konsekvens är signifikant högre för de hotbeskrivningar där aktören är specificerad som främmande makt. Därmed bekräftades hypotesen. Medelvärdet är 3,5 för de hotbeskrivningar där aktören är specificerad som främmande makt respektive 3,28 för de hotbeskrivningar där aktören inte är specificerad som främmande makt.

5) *När aktören specificeras som främmande makt bedömer respondenter som är vana vid att genomföra säkerhetsanalyser konsekvensen som högre.*

För respondenter som är vana vid att genomföra säkerhetsanalyser är bedömningarna av konsekvens signifikant högre för de hotbeskrivningar där aktören är specificerad som främmande makt. Därmed bekräftades hypotesen. Med respondenter som är vana vid att genomföra säkerhetsanalyser avses de som svarade 4 eller 5 på den femgradiga skalan för frågan kopplad till huruvida de

genomför säkerhetsanalyser inom ramen för sitt arbete. Medelvärdet är 3,46 för de hotbeskrivningar där aktören är specificerad som främmande makt respektive 3,18 för de hotbeskrivningar där aktören inte är specificerad som främmande makt.

6) *Specificerad aktör ger högre samstämmighet i bedömningarna av konsekvens än när aktören är ospecificerad.*

Samstämmigheten[6] i bedömningarna av konsekvens är högre för de hotbeskrivningar där en aktör är specificerad än när ingen aktör är specificerad. När alla respondenter beaktas är resultaten vid beräkning av Krippendorff's alpha (KA-värdena) 0,3442 (KI 0,2641–0,4208) när en aktör är specificerad respektive 0,2692 (KI 0,1877–0,3480) när ingen aktör är specificerad. Då skillnaden inte är statistiskt signifikant finns det inget generellt stöd för hypotesen.

7) *Samstämmigheten i bedömningarna av konsekvens är högre för respondenter med hög expertis än för respondenter med låg expertis.*

Avseende bedömningen av konsekvens är respondenter med hög expertis signifikant mer samstämmiga än respondenter med låg expertis. Därmed bekräftades hypotesen. KA-värdena är 0,3918 (KI: 0,3160–0,4608) för respondenter med hög expertis och 0,2754 (KI: 0,1969–0,3497) för respondenter med låg expertis, vilket innebär att det finns en signifikant skillnad trots att konfidensintervallen överlappar. Respondenter med hög respektive låg expertis avser de respondenter för vilka svaren avseende arbetar med informationssäkerhet, genomför säkerhetsanalyser och genomför informationsklassificering tillsammans överstiger 10 respektive understiger 7.

8) *Samstämmigheten i bedömningarna av konsekvens är högre för de respondenter som är säkra på sina bedömningar än för de respondenter som är osäkra på sina bedömningar.*

De respondenter som är säkra på sina bedömningar av konsekvens är signifikant mer samstämmiga än de respondenter som är osäkra på sina bedömningar av konsekvens. Därmed bekräftades hypotesen. KA-värdena är 0,3785 (KI: 0,3099–0,4486) respektive 0,2040 (KI: 0,1153–0,2802). Med respondenter som är säkra på sina bedömningar avses de som svarade 4 eller 5 på frågan kopplad till visshet avseende sina bedömningar av konsekvens. Med respondenter som är osäkra på sina bedömningar avses de som svarade 1 eller 2 på frågan kopplad till visshet avseende sina bedömningar av konsekvens.

[6] Som mått för samstämmighet används Krippendorff's alpha (KA).

9) *Samstämmigheten i bedömningarna av konsekvens är högre när hotbeskrivningen inkluderar resultatet av en informationsklassificering för tillgången.*

Samstämmigheten mellan bedömningarna av konsekvens är signifikant högre för hotbeskrivningar som inkluderar resultatet av en informationsklassificering för tillgången än för hotbeskrivningar som inte gör det. Därmed bekräftades hypotesen. KA-värdena för alla bedömare tillsammans är 0,5333 (KI: 0,4765–0,5872) när resultatet av en informationsklassificering för tillgången är specificerat respektive 0,1900 (KI: 0,0968–0,2715) när det inte är specificerat.

5.3.2 Test av hypoteser relaterade till bedömningen av sannolikhet

I detta avsnitt testas de hypoteser som relaterar till respondenternas bedömning av sannolikhet. För att testa hypotes 10, 11 och 12 jämförs erhållna medelvärden för de hotbeskrivningar där specificeringen av aktör skiljer sig mellan enkät A och enkät B. Denna skillnad finns mellan nio av de tio hotbeskrivningarna i enkäterna. För de hypoteser där ingen signifikant skillnad framkommit redovisas inte de framräknade konfidensintervallen.

10) *Bedömningen av sannolikhet påverkas av specificerad aktör.*

För alla respondenter visar genomförda tester på att det saknas signifikanta skillnader mellan medelvärdena för de bedömningar av sannolikhet som har gjorts för de två versionerna av varje hotbeskrivning. Därmed finns det inte något stöd för hypotesen.

11) *För respondenter som inte är säkra på sina bedömningar påverkas bedömningen av sannolikhet av specificerad aktör.*

Även för de respondenter som inte är säkra på sina bedömningar av sannolikhet visar genomförda tester på att det saknas signifikanta skillnader mellan medelvärdena för de bedömningar av sannolikhet som har gjorts för de två versionerna av varje hotbeskrivning. Därmed finns det inte något stöd för hypotesen. En respondent anses inte vara säker på sina bedömningar av sannolikhet om denne svarade 1 eller 2 på den femgradiga skalan tillhörande frågan om visshet avseende bedömningarna av sannolikhet.

12) *För respondenter som är säkra på sina bedömningar påverkas bedömningen av sannolikhet av specificerad aktör.*

Även för de respondenter som är säkra på sina bedömningar av sannolikhet visar genomförda tester på att det saknas signifikanta skillnader mellan medelvärdena för de bedömningar av sannolikhet som har gjorts för de två versionerna av varje hotbeskrivning. Därmed finns det inte något stöd för hypotesen. En respondent anses vara säker på sina bedömningar av sannolikhet om denne svarade 4 eller 5

på den femgradiga skalan tillhörande frågan om visshet avseende bedömningarna av sannolikhet.

13) *När aktören specificeras som främmande makt bedöms sannolikheten som högre.*

Det finns ingen signifikant skillnad mellan medelvärdena för bedömningarna av sannolikhet för de hotbeskrivningar där aktören är specificerad som främmande makt än när aktören inte är specificerad som främmande makt. Därmed finns det inte något stöd för hypotesen. Medelvärdet är 2,95 och identiskt för de två uppsättningarna med hotbeskrivningar.

14) *När aktören specificeras som främmande makt bedömer respondenter som är vana vid att genomföra säkerhetsanalyser sannolikheten som högre.*

För respondenter som är vana vid att genomföra säkerhetsanalyser finns inga signifikanta skillnader avseende bedömningarna av sannolikhet för de hotbeskrivningar där aktören är respektive inte är specificerad som främmande makt. Därmed finns det inte något stöd för hypotesen. Med respondenter som är vana vid att genomföra säkerhetsanalyser avses de som svarade 4 eller 5 på den femgradiga skalan för frågan kopplad till huruvida de genomför säkerhetsanalyser inom ramen för sitt arbete. Medelvärdet är 3,04 för de hotbeskrivningar där aktören är specificerad som främmande makt respektive 2,94 för de hotbeskrivningar där aktören inte är specificerad som främmande makt.

15) *Specificerad aktör ger högre samstämmighet i bedömningarna av sannolikhet än när aktören är ospecificerad.*

Det finns inga samband i insamlade data som visar på att specificerad aktör ger högre samstämmighet i bedömningarna av sannolikhet. Därmed finns det inte något stöd för hypotesen. Tvärtom indikerar resultaten att samstämmigheten sjunker när aktören är specificerad, men inga av skillnaderna är signifikanta. För alla bedömare tillsammans är KA-värdena 0,1417 (KI: 0,0406–0,2297) när aktören är specificerad respektive 0,2602 (KI: 0,1749–0,3422) när det inte finns någon specificerad aktör.

16) *Samstämmigheten i bedömningarna av sannolikhet är högre för respondenter med hög expertis än för respondenter med låg expertis.*

Respondenter med hög expertis har högre samstämmighet i sina bedömningar av sannolikhet än respondenter med låg expertis. Skillnaden är dock inte signifikant. Därmed finns det inte något stöd för hypotesen. För respondenter med hög

expertis är KA-värdet 0,2221 (KI: 0,1269–0,3097), medan KA-värdet för respondenter med låg expertis är 0,1721 (KI: 0,0807–0,2625).

17) *Samstämmigheten i bedömningarna av sannolikhet är högre för de respondenter som är säkra på sina bedömningar än för de respondenter som är osäkra på sina bedömningar.*

De som är säkra på sina bedömningar har högre samstämmighet i sina bedömningar än de som är osäkra på sina bedömningar, men skillnaden är inte signifikant. Därmed finns det inte något stöd för hypotesen. För de som är säkra på sina bedömningar är KA-värdet 0,2110 (KI: 0,1223–0,3000), medan KA-värdet för de som är osäkra på sina bedömningar är 0,1744 (KI: 0,0797–0,2585). Med respondenter som är säkra på sina bedömningar avses de som svarade 4 eller 5 på frågan kopplad till visshet avseende sina bedömningar av sannolikhet. Med respondenter som är osäkra på sina bedömningar avses de som svarade 1 eller 2 på frågan kopplad till visshet avseende sina bedömningar av sannolikhet.

18) *Samstämmigheten i bedömningarna av sannolikhet är högre när hotbeskrivningen inkluderar resultatet av en informationsklassificering för tillgången.*

Samstämmigheten mellan bedömningarna av sannolikhet är signifikant högre för hotbeskrivningar som inkluderar resultatet av en informationsklassificering för tillgången. Därmed bekräftades hypotesen. KA-värdena för alla respondenter tillsammans är 0,3885 (KI: 0,3124–0,4595) när resultatet av en informationsklassificering för tillgången är specificerat respektive 0,0801 (KI: -0,0296–0,1731) när det inte är specificerat. Denna signifikanta skillnad återfinns också för grupperna med hög respektive låg expertis, de som är säkra på sina bedömningar och de som är osäkra på sina bedömningar.

5.3.3 Test av hypoteser relaterade till både sannolikhet och konsekvens

19) *Samstämmigheten är högre vid bedömningar av konsekvens än vid bedömningar av sannolikhet.*

Samstämmigheten mellan bedömningarna av konsekvens för alla hotbeskrivningarna är signifikant högre än samstämmigheten mellan bedömningarna av sannolikhet för alla hotbeskrivningarna. Därmed bekräftades hypotesen. KA-värdena är 0,3558 (KI: 0,2782–0,4229) avseende bedömningarna av konsekvens respektive 0,2216 (KI: 0,1338–0,3123) avseende bedömningarna av sannolikhet. Denna signifikanta skillnad återfinns också för gruppen med hög expertis, även när endast hotbeskrivningar som saknar resultat av en informationsklassificering för tillgången beaktades.

20) Korrelationen mellan bedömningarna av sannolikhet och konsekvens är negativ.

Det finns inte någon signifikant korrelation[7] mellan bedömningarna av sannolikhet och konsekvens. Därmed finns det inte något stöd för hypotesen.

5.3.4 Informationselementens gemensamma betydelse för bedömningen

För att testa informationselementens betydelse för respondenternas bedömningar av sannolikhet och konsekvens formulerades regressionsmodeller med sannolikhet respektive konsekvens som beroende variabel samt aktör, tillgång, oönskad händelse, skyddsåtgärd och tillvägagångssätt som oberoende variabler. Regressionsmodellerna ska alltså estimera respondenternas sannolikhets- och konsekvensbedömningar utgående ifrån hur informationselementen aktör, tillgång, oönskad händelse, skyddsåtgärd och tillvägagångssätt har beskrivits.

För att modellera beskrivningen av informationselementen grupperades de använda formuleringarna i kategorier, vilka sedan användes för att representera informationselementen i regressionsmodellerna. Från de 19 hotbeskrivningarna[8] identifierades nio kategorier för aktör, fyra kategorier för tillgång, två kategorier för oönskad händelse, två kategorier för skyddsåtgärd och fyra kategorier för tillvägagångssätt.

De i regressionsmodellerna ingående oberoende variablerna är nominala, dvs. det går inte att säga att något av de möjliga värdena för en variabel är större eller mindre än något av de andra möjliga värdena för denna variabel. Därmed måste de oberoende variablerna kodas med var sin uppsättning med s.k. dummyvariabler (eng. dummy variables) som representerar de oberoende variablernas möjliga värden, vilket i det här fallet innebär att motsvarande kategori har använts för att beskriva informationselementet i den aktuella hotbeskrivningen. Denna kodning refereras ofta till som dummy coding (Warner, 2013).

För att testa vilka informationselement som är signifikanta formulerades en fullständig regressionsmodell med alla tillgängliga dummyvariabler, vilka var och en representerar att en kategori används för att specificera ett informationselement. Från den fullständiga regressionsmodellen togs därefter de delmängder av dummyvariablerna som motsvarar vart och ett av informationselementen bort från modellen. På så sätt fastställs de modellerade

[7] Enligt test med *Pearsons produktmomentkorrelationskoefficient* och *Spearmans rangkorrelationskoefficient*.

[8] Enkät A och enkät B innehöll var för sig nio unika hotbeskrivningar och en gemensam, vilket resulterade i totalt 19 unika hotbeskrivningar.

informationselementens bidrag till förklarad varians[9], vilket ger indikationer på de olika informationselementens påverkan på bedömningarna av sannolikhet och konsekvens.

Regressionsmodellen för sannolikhet förklarar cirka 20 % av variansen, med signifikanta bidrag från aktör, tillgång, oönskad händelse, skyddsåtgärd och tillvägagångssätt. Regressionsmodellen för konsekvens förklarar cirka 35 % av variansen, med signifikanta bidrag från aktör, tillgång och tillvägagångssätt. Det innebär att regressionsmodellen för bedömning av konsekvens fungerar nästan lika bra som regressionsmodellerna som har tagits fram för att skatta respondenters intention att följa informationssäkerhetsbestämmelser (Sommestad, Karlzén och Hallberg, 2015). Regressionsmodellen för bedömning av sannolikhet fungerar dock betydligt sämre.

För att testa vilka av de kategorier, dvs. dummyvariabler, som används för att koda de informationselement som är signifikanta formulerades regressionsmodeller stegvis, vilket innebär att dummyvariabler som ingår i modellen tas bort om de inte ger signifikanta bidrag och dummyvariabler som inte ingår i modellen tas in i modellen om de ger signifikanta bidrag[10].

Den resulterande regressionsmodellen för sannolikhet inkluderar dummyvariablerna motsvarande de kategorier som återfinns i Tabell 10. I tabellen framgår även dummyvariablernas påverkan på estimaten av sannolikhetsvärdena (som ligger på skalan 1 till 5). Exempelvis höjer tillgångskategorin *öppen information* sannolikhetsestimatet drygt ett steg och tillvägagångssättskategorin *skadlig kod* sänker sannolikhetsestimatet med drygt ett halvt steg.

Tabell 10: Kategorier för beskrivning av informationselement som ingår i regressionsmodell för sannolikhet samt deras påverkan på de estimerade värdena.

Informationselement	**Kategori**	**Påverkan**
Tillgång	Öppen information	1,021
Tillvägagångssätt	Stöld	-1,036
	Insider	-0,939
	Skadlig kod	-0,582
Oönskad händelse	Tillgänglighet	-0,565

[9] För att bygga regressionsmodellen i SPSS användes kommandot *regression* tillsammans med metoden *test*, som anges med subkommandot *method*.

[10] För att bygga regressionsmodellen i SPSS användes kommandot *regression* tillsammans med metoden *stepwise* (som anges med subkommandot *method*).

Informationselement	Kategori	Påverkan
Aktör	Tulltjänsteman	-0,551
	Utländsk försvarsindustri	0,378
	Kriminella	0,229

Den resulterande regressionsmodellen för konsekvens inkluderar dummyvariablerna motsvarande de kategorier som återfinns i Tabell 11. I tabellen framgår även dummyvariablernas påverkan på estimaten av konsekvensvärdena (som ligger på skalan 1 till 5). Exempelvis höjer tillgångskategorin *hemlig/secret information* konsekvensestimatet med över ett steg medan skyddsåtgärdskategorin *specificerad*, vilken innebär att det finns en specificerad skyddsåtgärd, sänker konsekvensestimatet med nästan ett steg.

Tabell 11: Kategorier för beskrivning av informationselement som ingår i regressionsmodell för konsekvens samt deras påverkan på de estimerade värdena.

Informationselement	Kategori	Påverkan
Tillgång	Hemlig/secret information	1,368
Skyddsåtgärd	Specificerad	-0,916
Tillvägagångssätt	Stöld	0,675
	Skadlig kod	0,649
Aktör	Forskare	0,432
	Anställd	0,381
	Aktivister	0,404

Regressionsmodellerna ger möjlighet att identifiera faktorer som är relevanta för respondenters bedömningar. Avseende regressionsmodellerna för bedömning av sannolikhet och konsekvens handlar det om kategorier som används vid klassificering av hotbeskrivningarnas innehåll. Det är dock vanskligt att fästa för stor betydelse vid att specifika kategorier *inte* kommer med i regressionsmodellen. Vissa kategorier kan samvariera och därmed täcka in varandra. Modellen innehåller dessutom en konstant. Detta medför, exempelvis, att om formuleringen av modellen resulterar i att denna konstant blir hög kommer vissa av de kategorier som ingår i högt bedömda hotbeskrivningar att fångas upp av konstanten.

Avseende skyddsåtgärder används endast två kategorier för att klassificera hotbeskrivningarna utifrån huruvida de innehåller en specificering av någon skyddsåtgärd eller ej. Att det finns en specificering av skyddsåtgärder sänker bedömningen med nästan ett steg på den femgradiga skalan för konsekvens. Detta resultat illustrerar en utmaning gällande tydlighet avseende gränsdragningen mellan skyddsåtgärder och vad som är den skyddsvärda tillgången. Om ett säkerhetsskåp innehåller hemliga handlingar, vad utgör den skyddsvärda tillgången, de hemliga handlingarna eller säkerhetsskåpet med innehåll? Om de som bedömer sannolikhet och konsekvens har olika uppfattning om vad som utgör den skyddsvärda tillgången kan det påverka deras respektive bedömningar av sannolikhet och konsekvens.

6 Diskussion

En central del i genomförandet av säkerhetsanalyser är bedömningen av sannolikhet och konsekvens för identifierade hot. Det underlag som används för att bedöma sannolikhet och konsekvens är en hotbeskrivning som ska formuleras för varje identifierat hot. Trots det saknas tydliga specifikationer av vad som ska ingå i dessa hotbeskrivningar för att de ska utgöra adekvata bedömningsunderlag.

Den uppsättning informationselement som presenteras i kapitel 4 är ett första förslag på vad som behöver ingå i en hotbeskrivning. Syftet är att förslaget ska utgöra en utgångspunkt för vidare diskussion och utveckling av kunskapen om vad som behöver ingå i en hotbeskrivning. Förslaget utgår ifrån de informationselement som har identifierats i H Säk Grunder, med förtydligandet att tillvägagångssättet lyfts ut från den oönskade händelsen till ett separat informationselement. Dessutom föreslås fem principer att följa när hotbeskrivningar ska utformas.

Samtidigt som de föreslagna informationselementen i sig ger en viss struktur för innehållet kan de föreslagna principerna för utformning nyttjas för att erhålla ensade beskrivningar där skillnader beror på hotbeskrivningars innehåll snarare än på deras utformning. På så sätt kan situationer undvikas där hotbeskrivningar med samma sakliga innehåll bedöms olika på grund av skillnader i deras utformning.

Den genomförda kvantitativa studien av hotbeskrivningars påverkan på bedömningar av sannolikhet och konsekvens visar att det underlag som det aktuella scenariot och hotbeskrivningarna ger är otillräckligt för att erhålla samstämmiga bedömningar, speciellt avseende sannolikhet. En svaghet i den genomförda studien är att scenariot utgår från en fiktiv organisation. När bedömningarna genomförs i kontext av den egna organisationen blir förutsättningarna annorlunda. En utmaning vid genomförandet av studier inom området är att data som kommer från skarpa analyser ofta anses vara känsliga. Samtidigt blir inte kunskapen gällande vilket innehåll en hotbeskrivning ska ha och hur de olika delarna ska utformas för att på bästa sätt stödja riskbedömningen bättre än vad resultaten från de genomförda studierna medger. Det behövs därmed studier som utgår ifrån riktiga scenarion och hotbeskrivningar som är relevanta i kontexten. Det kan dock noteras att samtidigt som samstämmigheten mellan respondenternas bedömningar var låg så ansåg de flesta respondenterna sig vara säkra[11] på sina bedömningar och ha nödvändig förkunskap.

Alla de signifikanta skillnader som berodde på specificeringen av aktör relaterar till bedömningen av konsekvens. Detta är anmärkningsvärt då bedömningen av konsekvens inte ska påverkas av vilken aktör som har specificerats. Dessa

[11] Fler respondenter valde 4 eller 5 än 1 eller 2 på den femgradiga skalan för de tre frågorna.

resultat kan ses som ett stöd för att konsekvensen ska bedömas innan aktören specificeras, vilket är fallet när säkerhetsanalyser genomförs i enlighet med H Säk Grunder.

Det är anmärkningsvärt att specificeringen av aktör inte visats ha någon signifikant påverkan på bedömningen av sannolikhet, trots att aktören enligt H Säk Grunder specificeras till stöd för bedömningen av sannolikhet. Denna brist på signifikanta skillnader kan bero på att det är svårt att bedöma sannolikhet alternativt att enkäternas scenario och hotbeskrivningar inte ger lika bra stöd för bedömningen av sannolikhet som för bedömningen av konsekvens. Tidigare arbeten indikerar att samstämmigheten är lägre vid bedömning av sannolikhet än vid bedömning av konsekvens (Hallberg, Bengtsson och Karlzén, 2016; Hallberg *m.fl.*, 2017), vilket antyder att det är svårare att bedöma sannolikhet än konsekvens. Resultaten från årets studie visar att samstämmigheten är signifikant högre vid bedömningar av konsekvens än vid bedömningar av sannolikhet. Denna slutsats gäller såväl vid beaktande av alla deltagande respondenters bedömningar som vid avgränsning till respondenter med hög expertis samt för respondenter med hög expertis även när endast hotbeskrivningar som saknar resultat av en informationsklassificering för tillgången beaktas.

En möjlig slutsats av att specificeringen av aktör inte påverkade bedömningarna av sannolikhet är att det inte är nödvändigt att inkludera aktören i de hotbeskrivningar som ligger till grund för bedömningar av sannolikhet. Med beaktande av att även samstämmigheten mellan bedömningarna av sannolikhet var låg är det troligare att aktören behöver specificeras tydligare för att få genomslag i bedömningarna av sannolikhet och hjälpa till att öka samstämmigheten.

Fortsatta studier kring bedömning av risker är en viktig del i vidareutvecklingen av förslaget avseende vilka informationselement som behövs i en hotbeskrivning samt hur denna hotbeskrivning ska utformas. Några exempel på frågeställningar som kan vara relevanta för fortsatta studier återges nedan.

- Vilka kopplingar finns mellan verksamhetsanalyser och säkerhetsanalyser och hur kan verksamhetsanalyser utformas för att ge bästa möjliga stöd till säkerhetsanalyserna? Verksamhetsanalysen ligger till grund för centrala delar av säkerhetsanalysen, såsom identifieringen av tillgångar, hur tillgångarna kan påverkas negativt (de oönskade händelserna), hur skadlig denna påverkan vore (konsekvenserna) och sårbarheter.
- Vilka ytterligare uppdelningar av informationselementen kan nyttjas för att erhålla bättre underlag för bedömningarna av sannolikhet och konsekvens? Resultaten från den genomförda enkätstudien visar inte på att specificeringen av aktör påverkar bedömningen av sannolikhet, vilket kan tolkas som att aktören behöver specificeras tydligare, exempelvis avseende kapacitet, intention och tillfälle.

7 Referenser

Adams, J. (1999) ”Risk, Freedom and Responsibility”, *In: The Risk of Freedom. Individual Liberty and the Modern World. Institute of United States Studies, University of London: London*. Institute of United States Studies, University of London, (1998), s. 33–58.

Alberts, C. och Dorofee, A. (2001) *OCTAVE Method Implementation Guide Version 2.0*. Pittsburgh, PA, USA.

Casey, T. (Intel I. T. (2007) ”Threat Agent Library Helps Identify Information Security Risks”, *Intel White Paper*, (September), s. 12.

Davis, A. *m.fl.* (1993) ”Identifying and Measuring Quality in a Software Requirements Specification”, i *First International Software Metrics Symposium*. Baltimore, Maryland: IEEE, s. 141–152.

Fenz, S. *m.fl.* (2014) ”Current challenges in information security risk management”, *Information Management & Computer Security*, 22(5), s. 410–430.

Försvarsmakten (2001) *Handbok för Försvarsmaktens Säkerhetstjänst, Informationsteknik Hotbeskrivning (H SÄK IT Hot)*. M7745-734051. Försvarsmakten.

Försvarsmakten (2006) *Handbok för Försvarsmaktens säkerhetstjänst, Hotbedömning (H Säk Hot)*. Stockholm: Försvarsmakten.

Försvarsmakten (2009a) *Försvarsmaktens gemensamma riskhanteringsmodell, Handbok*. M7739-350012. Försvarsmakten.

Försvarsmakten (2009b) *Handbok bedömning antagonistiska hot: komplement till Försvarsmaktens gemensamma riskhanteringsmodell 2009, M7739-350013*. Försvarsmakten.

Försvarsmakten (2013) *Handbok Säkerhetstjänst Grunder (H Säk Grunder)*. M7745-734011. Försvarsmakten.

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

Försvarsmakten (2015) *Handbok Målsättningsarbete Tekniska system (H Mål Tek Syst 2015)*.

Hallberg, J. *m.fl.* (2017) ”The Significance of Information Security Risk Assessments Exploring the Consensus of Raters’ Perceptions of Probability and Severity”, *International conference on Security and Management*, s. 131–137.

Hallberg, J., Bengtsson, J. och Karlzén, H. (2016) *Beskriva och bedöma hot mot IT-system – Varför är det så svårt?* FOI-R--4330--SE. Totalförsvarets forskningsinstitut, FOI.

Hansson, J., Granlund, H. och Hallberg, N. (2011) *Att uttrycka krav i materielmålsättningar – Formulera och granska*. FOI-R--3250--SE. Totalförsvarets forskningsinstitut, FOI.

Hayes, A. F. och Krippendorff, K. (2007) ”Answering the Call for a Standard Reliability Measure for Coding Data”, *Communication Methods and Measures*, 1(1), s. 77–89. doi: 10.1080/19312450709336664.

ISO/IEC (2011) *ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management*.

Korman, M. *m.fl.* (2014) ”Overview of Enterprise Information Needs in Information Security Risk Assessment”, i *18th IEEE International Enterprise Distributed Object Computing Conference (EDOC)*, s. 42–51. doi: 10.1109/EDOC.2014.16.

Krippendorff, K. (2011) ”Computing Krippendorff’s Alpha-Reliability”, *Departmental Papers (ASC)*, s. 12.

Ministerio de Administraciones Públicas (2006) ”MAGERIT version 2 – Methodology for Information Systems Risk Analysis and Management – II - Catalogue of Elements”, *Risk Analysis*, (June). doi: 326-06-044-8.

Ministry of Finance and Public Administration (2014) *MAGERIT - version 3.0. Methodology for Information Systems Risk Analysis and Management - The Method*.

NIST (2012) *NIST Special Publication 800-30, Revision 1: Guide for Conducting Risk Assessments*. Gaithersburg, MD, USA: National Institute of Standards and Technology.

Opdahl, A. L. och Sindre, G. (2009) ”Experimental comparison of attack trees and misuse cases for security threat identification”, *Information and Software Technology*. Elsevier B.V., 51(5), s. 916–932. doi: 10.1016/j.infsof.2008.05.013.

Parker, D. B. (2012) ”Toward a New Framework for Information Security?”, i *Computer Security Handbook*. Hoboken, NJ, USA: John Wiley & Sons, Inc., s. 3.1-3.23. doi: 10.1002/9781118851678.ch3.

Schneier, B. (2000) *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons, Inc. New York, NY, USA.

Shanteau, J. (2015) ”Why task domains (still) matter for understanding expertise”, *Journal of Applied Research in Memory and Cognition*, 4(3), s. 169–175.

SIS (2015) *SIS-TR 50:2015 – Terminologi för informationssäkerhet*. Teknisk rapport, SIS-TR 50:2015.

Sommestad, T., Karlzén, H. och Hallberg, J. (2015) ”A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour”, *International Journal of Information Security and Privacy*. IGI Global, 9(1), s. 26–46.

The Standish Group International (1994) *The CHAOS Report*,

https://standishgroup.com/sample_research_files/chaos_report_1994.pdf.

Warner, R. M. (2013) *Applied Statistics: From Bivariate Through Multivariate Techniques*. 2:a uppl. SAGE Publications, Inc.

Att bedöma sannolikheter och konsekvenser är en central del i genomförandet av säkerhetsanalyser inom Försvarsmakten. Vid systematiskt arbete med säkerhetsanalyser ligger skriftliga beskrivningar av identifierade hot till grund för dessa bedömningar. Det saknas dock till stor del kunskap om hur dessa hotbeskrivningars innehåll och utformning påverkar bedömningarna av sannolikhet och konsekvens.

För att stödja framtagandet av hotbeskrivningar som utgör adekvat underlag för riskbedömningar presenteras i denna rapport ett förslag avseende vad en hotbeskrivning ska innehålla och hur den ska utformas. Till grund för innehållet presenteras en uppsättning med informationselement som ska ingå i en hotbeskrivning. Till stöd för utformningen av hotbeskrivningar presenteras även en uppsättning med principer som bör följas. Förslaget är inte avsett att utgöra en slutlig version utan ska beaktas som en utgångspunkt för vidare diskussion och utveckling av kunskapen om vad som behöver ingå i en hotbeskrivning och hur den ska utformas.

Som ett första steg i att utvärdera den föreslagna uppsättningen informationselement som utgör en hotbeskrivning genomfördes en kvantitativ enkätstudie. Studien utformades för att undersöka vilken påverkan specificeringen av aktör har på bedömningen av sannolikhet och konsekvens för ett hot. Resultaten från studien visar bland annat att det finns en stor variation mellan olika respondenter med avseende på hur de bedömer sannolikhet och konsekvens utgående från identiska hotbeskrivningar.

FOI

ISSN 1650-1942

www.foi.se