Institutionen för kommunikation och information
Examensarbete i datalogi 15hp
C-nivå
Vårterminen 2009

Lönsamhet vid investering i intrångsdetekteringssystem

Hur beräknas den?

Jonas Svensson

Lönsamhet vid investering i intrångsdetekteringssystem

Examensrapport inlämnad av Jonas Svensson till Högskolan i Skövde, för Kandidatexamen (B.Sc.) vid Institutionen för kommunikation och information. Arbetet har handletts av Marcus Nohlberg.

2009-06-18

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

Lönsamhet vid investering i intrångsdetekteringssystem

Jonas Svensson

Sammanfattning

Denna rapport syftar till att ge en inblick i hur lönsamhet för investering i intrångsdetekteringssystem kan beräknas. Rapporten visar hur tre olika beräkningsmodeller kan användas för att bedöma investeringar i intrångsdetekteringssystem. I resultatet för rapporten presenteras hur modellerna fungerar, datainsamlingen för modellerna berörs och beräkningsexempel demonstreras för var och en av modellerna. Från de tre beräkningsmodellerna har även ett enklare interaktivt verktyg tagits fram, vilket skall kunna användas för att göra beräkningar med de olika modellerna. Verktyget presenteras också i rapporten. Då rapporten fokuserar på intrångsdetekteringssystem ges också en enklare förklaring för dessa.

Slutsatserna för rapporten blev bland annat att beräkningsmodellerna går att använda för att lönsamhetsbedöma investeringar i IDS, att en investering i IDS är lönsam om beräkningsmodellerna ger positiva resultat samt att insamlingen av data till modellerna är en besvärlig fas. I diskussionen för rapporten diskuteras bland annat svårigheterna i datainsamlingen och nyttan med beräkningsmodellerna.

Nyckelord: Intrångsdetekteringssystem, beräkningsmodell, lönsamhet, investering

Innehållsförteckning

1 Introduktion 1

2 Bakgrund 3

2.1 Intrångsdetekteringssystem (IDS) 3

2.1.1 Signaturbaserad 3

2.1.2 Avvikelsebaserat 3

2.1.3 Hybrid- eller sammansatt detektering 4

2.1.4 Eventualiteter 4

2.1.5 Nätverksbaserade samt värdbaserade IDS 4

2.1.6 Problem och utmaningar 5

2.1.7 Fördelar och nackdelar 5

2.2 Beräkningsmodeller 5

2.2.1 Avkastning på investering (ROI) 6

2.2.2 ”Net present value” (NPV) 6

2.2.3 “Internal rate of return” (IRR) 6

2.2.4 Total ägandekostnad (TCO) 7

2.2.5 Svagheter och nackdelar i ROI, NPV samt IRR 7

2.3 Relaterade arbeten 7

3 Problemprecisering 9

3.1 Bakgrund 9

3.2 Frågeställning 9

4 Metod 11

4.1 Litteratursökning 11

4.2 Interaktiva verktyg 11

4.3 Metodval 11

5 Tillvägagångssätt 13

6 Resultat 14

6.1 ROSI 14

6.2 NPV 15

6.3 IRR 15

6.4 Datainsamling 16

6.5 Exempel 17

6.5.1 Beräkning med ROSI 17

6.5.2 Beräkning med NPV 18
6.5.3 Beräkning med IRR 19
6.5.4 Sammanfattning 19
6.6 Kostnadseffektivitet samt kostnadsmodeller 19
6.7 Interaktivt verktyg 20
7 Diskussion 23
7.1 Metod 23
7.2 Resultat 23
8 Slutsats 27
9 Förslag till fortsatt arbete 29
Referenser 30
Bilaga A – Förkortningar 1

1 Introduktion

Internet är idag ett stort medium. Alla utnyttjar Internet till allt från att skicka e-post till att sköta bankärenden. I takt med att Internet växer som medium för kommunikation och handel ökar dock hoten från spammare, angripare samt kriminella företagsamheter (Patcha & Park, 2007). ”Computer security institute” (CSI) har de senaste tretton åren gjort undersökningar bland företag och organisationer i USA angående nätverksäkerhet samt datasäkerhet. I undersökningen för år 2008 svarade 43 % av 517 svarande att de hade haft säkerhetsincidenter (Richardson, 2008). En annan fråga i undersökningen handlar om ett antal olika datorbaserade attacker samt incidenter. Från de 433 svarande går det att utläsa att de fyra vanligaste incidenterna är virus (50 %), missbruk från insidan (44 %), stöld av bärbara datorer (42 %) samt otillåten access (29 %).

Undersökningen från CSI tar också upp vilka skyddsmekanismer som används av företagen och organisationerna. Av 521 svarande använder de allra flesta antivirusprogram (97 %) samt brandväggar (94 %). En relativt stor del av de tillfrågade (69 %) använder så kallade intrångsdetekteringssystem (IDS). IDS är cyberrymdens svar på inbrottslarm och är tillsammans med brandväggar en av de fundamentala teknikerna för säkerhet i nätverk (Patcha & Park, 2007). Ett IDS samlar in information från olika områden i ett nätverk eller en dator. Den insamlade informationen används sedan för att identifiera möjliga säkerhetsintrång. Ett annat sätt att beskriva IDS är att de skall identifiera handlingar som äventyrar sekretessen, integriteten eller tillgängligheten av ett nätverk/system. IDS är kapabla att upptäcka olika slag av skadlig trafik på nätverket samt skadligt datoranvändande. Bland annat skall nätverksattacker mot sårbara system, databaserade attacker, värdbaserade attacker samt sabotageprogram kunna upptäckas (Patcha & Park, 2007).

Ett företag som bestämmer sig för att införskaffa ett IDS behöver bland annat fundera över lönsamheten i ett sådant projekt. Att införskaffa ett IDS kostar pengar och det finns en mängd aspekter att fundera över. Vad är det som kostar och hur mycket kostar det? Två exempel på kostnader är kostnad för själva IDS:et (om det inte är open source) och kostnad för driften av IDS:et. Det gäller också att veta vad det kostar att inte införskaffa ett IDS. Att inte investera i ett IDS kommer troligtvis innebära att x antal säkerhetsincidenter kommer inträffa, vilket i sin tur leder till en viss kostnad. Det gäller sedan att jämföra den förväntade kostnaden utan IDS med den förväntade kostnaden med IDS. Om kostnaden utan IDS är större än kostnaden med IDS är det troligtvis lönsamt att investera i IDS. och tvärtom.

Syftet med denna rapport är att presentera tre olika beräkningsmodeller som kan användas för att bedöma huruvida en investering i IDS är lönsam eller ej. Rapporten tar också upp en del om vad det är som kostar vid en investering och hur dessa kostnader kan beräknas och uppskattas. I rapporten ges också en enklare redogörelse för IDS.

Rapporten riktar sig i första hand till läsare som är intresserade av IDS och hur lönsamheten i investering i IDS kan beräknas. Rapporten riktar sig även till dem som är allmänt intresserade av hur investeringar i informationssäkerhet kan lönsamhetsbedömas.

Strukturen i rapporten ser ut på följande vis: I avsnitt 2 ges en enklare beskrivning av IDS och beräkningsmodeller. Därefter preciseras och definieras problemet samt frågeställning i avsnitt 3. Avsnitt 4 och 5 beskriver metod och tillvägagångssätt.

Resultatet presenteras i avsnitt 6 och där ges både beskrivning samt beräkningsexempel till beräkningsmodellerna. I avsnitt 7 diskuteras metod samt resultat och i avsnitt 8 dras ett antal slutsatser utifrån de definierade problemen. Rapporten avslutas med referensredovisning. Då rapporten innehåller en mängd förkortningar finns dessa tillgängliga i Bilaga A.

2 Bakgrund

Detta avsnitt delas upp i tre delar. Första delen handlar om IDS och ger en övergripande förklaring för IDS. Andra delen ger en enkel introduktion till beräkningsmodeller. Avsnittet avslutas med att relaterade arbeten tas upp.

2.1 Intrångsdetekteringssystem (IDS)

IDS är ett verktyg för att skydda nätverk och datorsystem. Patcha & Park (2007) definierar IDS som ett mjukvaruverktyg för att upptäcka otillåten access till ett datorsystem eller nätverk. Axelsson (2000a) använder en annan analogi för att förklara, och kallar IDS för datorsäkerhetens inbrottslarm.

IDS är kapabla att upptäcka olika slag av skadlig trafik på nätverket samt skadligt datoranvändande. Bland annat skall nätverksattacker mot sårbara system, databaserade attacker, värdbaserade attacker samt sabotageprogram kunna upptäckas (Patcha & Park, 2007). Ett IDS består bland annat av en enhet som samlar in information om det övervakade systemet. Den insamlade informationen analyseras av en detektor, varpå IDS:et larmar om en överträdelse eller misstänkt aktivitet upptäcks. Larmet skickas till en säkerhetsansvarig som sedan avgör vad som skall göras (Axelsson, 2000a). Enligt Patcha & Park (2007) är processen med analys samt detektion själva hjärtat i IDS:et, och det är också där algoritmerna för att upptäcka misstänkta aktiviteter återfinns.

Både Axelsson (2000a) och Patcha & Park (2007) talar om tre olika typer av detekteringsalgoritmer: signaturbaserad detektering, avvikelsebaserad detektering samt hybrid/sammansatt detektering. Alla dessa tre tekniker fungerar på olika sätt samt skiljer sig vad det gäller för och nackdelar.

2.1.1 Signaturbaserad

En signatur kan vara ett simpelt mönster som skall matchas mot paketen som skickas i nätverket (Zhengbing, et al., 2008). I signaturbaserad detektering samlas signaturer av kända attacker in. Signaturerna för attacker används sedan i IDS:et. Där kontrolleras de mot filer och aktiviteter för att undersöka om några signaturer finns på nätverket eller i datorerna. Är det några signaturer närvarande innebär det att IDS:et har upptäckt en attack (Ye, et al., 2006). Ye, et al. (2006) ger ett exempel där tre på varandra följande misslyckade inloggningsförsök lagras som en signatur för gissningsattack med mål att knäcka lösenord.

Kända attacker kan upptäckas med ganska få falska alarm vilket är en fördel för signaturbaserad detektering. Det går också att vända på det och säga att nackdelen är att icke kända attacker ej går att upptäcka, och att signaturerna hela tiden måste uppdateras (Patcha & Park, 2007).

2.1.2 Avvikelsebaserat

I avvikelsebaserad detektering skapas en normalitetsprofil för vad som är normalt beteende i systemen. Normalitetsprofiler kan t ex skapas genom att samla in data under normala omständigheter för systemen. Vid övervakning av datorerna och nätverket används normalitetsprofilen för att undersöka om det finns aktiviteter som skiljer sig mot det normala beteendet. Om en stor skillnad upptäcks i ett pågående beteende jämfört mot det normala kan det vara en möjlig attack (Ye, et al., 2006). Ye, et al. (2006) ger återigen ett exempel. En normalitetsprofil kan skapas för en

webbserver med sekvenser av förväntade användaraktiviteter. Om en sekvens skiljer sig mot de förväntade sekvenserna kan det vara en attack.

Jämfört med signaturbaserad detektering har avvikelsebaserad detektering möjlighet att upptäcka icke kända attacker, vilket är en fördel. En nackdel med avvikelsebaserade IDS är att sådana system kan lida av många falska alarm. Detta eftersom avvikelsebaserade IDS letar efter onormala aktiviteter snarare än attacker (Patcha & Park, 2007).

2.1.3 Hybrid- eller sammansatt detektering

Hybriddetektering kombinerar signaturbaserad samt avvikelsebaserad detektering. Hybriddetektering tar beslut via en ”hybridmodell” och system som använder hybriddetektering kan ses som signaturinspirerade IDS. Den ”hybrida modellen” är baserad på både normala aktiviteter i systemet och inkräktande aktiviteter från angripare (Patcha & Park, 2007).

I ett test utfört av Depren, et al. (2005) kombinerades ett avvikelsebaserat IDS med ett signaturbaserat IDS för att fungera som en hybridlösning. Resultatet blev att den hybrida lösningen hade en detekteringsgrad på 99,90 %. Det jämfördes bland annat mot att enbart använda det avvikelsebaserade IDS:et, vilket gav en detekteringsgrad på 98,96. Enligt Depren, et al. gav den föreslagna hybrida lösningen bättre prestanda än de individuella lösningarna. Patcha & Park (2007) menar dock att de hybrida lösningarna inte alltid är bättre. Olika IDS fungerar på olika sätt, vilket enligt Patcha & Park gör att den största utmaningen med att skapa hybrida IDS är få de olika teknikerna att fungera effektivt.

2.1.4 Eventualiteter

Ett intrång behöver inte alltid klassas som en avvikelse. Det finns fyra eventualiteter (Patcha & Park, 2007):

- Falska negativa – Intrång som klassas som normala av IDS:et ses som falska negativa då de inte upptäcks.
- Falska positiva – Aktiviteter som ses som avvikande, men som inte är intrång, ses som falska positiva då IDS:et kommer larma för dem.
- Sanna negativa – Aktiviteter som ej är avvikande samt ej klassas som intrång är sanna negativa och dessa kommer IDS:et inte larma för.
- Sanna positiva – Aktiviteter som är intrång och som rapporteras av IDS:et som intrång klassas som sanna positiva.

2.1.5 Nätverksbaserade samt värdbaserade IDS

IDS kan även delas upp i två kategorier, ”network-based” IDS (NIDS) samt ”host-based” IDS (HIDS). NIDS används för att övervaka ett antal värddatorer i ett nätverkssegment. NIDS:et granskar trafiken från nätverket samt loggar från värddatorerna för att identifiera intrång (Kanlayasiri & Sanguanpong, 2002).

Ett HIDS används för att övervaka en specifik dator. På datorn som HIDS:et återfinns kan det övervaka specifika filer, loggar samt register. HIDS:et kan larma t ex vid modifiering av ett övervakat objekt (Sobh, 2006). Enligt Zhang, et al. (2003) förlitar sig ett HIDS på loggar från operativsystemet för att övervaka samt analysera de händelser som användare och applikationer genererar på den specifika datorn.

En huvudsaklig skillnad mellan NIDS och HIDS är att NIDS:et är ansvarigt för hela nätverket. HIDS:et däremot är bara ansvarigt för den specifika dator som det övervakar (Labib, 2004).

2.1.6 Problem och utmaningar

Det finns en mängd problem och utmaningar för IDS. Patcha & Park (2007) tar upp ett antal utmaningar som finns för nästa generations IDS. Framför allt menar Patcha & Park att det gäller avvikelsebaserade IDS.

Det första problemet som Patcha & Park berör är att traditionella IDS inte anpassats på ett sätt att de kan skydda t ex trådlösa nätverk. Detsamma gäller även nätverk med hastigheter för Gbit samt terabit. Ett annat problem som Patcha & Park tar upp är de falska alarm som IDS genererar. I en utvärdering av Newman, et al. (2002) undersöktes sju kommersiella IDS och ett IDS baserat på öppen källkod. Bland annat kom de fram till att:

- Flera av de undersökta IDS:en kraschade upprepade gånger på grund av bördan av alla falska alarm.
- När väl riktiga attacker inträffade misslyckades några av IDS:en att upptäcka dem, meddans en del IDS begravde rapporterna om attacker så djupt bland de falska alarmen att de var svåra att hitta.

För att ett IDS skall vara effektivt bör det inte ske mer än 1 falskt alarm för 100 000 händelser (Axelsson, 2000b). Enligt Patcha & Park är utmaningen med att minska den höga andelen av falska alarm en av de största och viktigaste att lösa.

Ytterligare problem och utmaningar som Patcha & Park tar upp är avsaknaden av att kunna utvärdera IDS, utmaningen i att skapa regler för att upptäcka interna attacker samt svårigheterna i att definiera vad som är normalt i ett nätverk.

2.1.7 Fördelar och nackdelar

Med den fakta som presenterats i avsnitt 2.1 – 2.1.5 är det inte svårt att inse att de företag som skall införskaffa ett IDS, eller redan har ett IDS i drift, ges både fördelar och nackdelar. Werlinger, et al. (2008) analyserar nio intervjuer med utövare inom IT-säkerhet som arbetat med IDS samt varit med och satt IDS i drift. De intervjuade har angivit både fördelar och nackdelar med IDS. Bland fördelarna som nämns återfinns identifiering av problem, övervakning med respekt för avskildheten för företagets personal, minskad tidspress för administratörer samt minskad ovisshet. Bland nackdelarna som nämns återfinns kostnaden, mängden arbete och tid som krävs, IDS:ets opålitlighet samt avsaknad av den egentliga nyttan med IDS.

2.2 Beräkningsmodeller

”Return on investment” (ROI), ”net present value” (NPV) samt ”internal rate of return” (IRR) är tre beräkningsmodeller för att beräkna kostnader och vinster vid investeringar i olika typer av projekt. Enligt Bojanc & Jerman-Blažič (2008) är ROI, NVP samt IRR dom för tillfället mest använda beräkningsmodellerna för att beräkna kostnader för investeringar i datorsäkerhet. Beräkningsmodellerna kan användas en och en eller kombineras. I CSI:s (Richardson, 2008) undersökning för 2008 har 44 % av 408 svarande angett att de använder ROI, 26 % att de använder NPV samt 23 % att de använder IRR. Det finns också en modell, ”total cost of ownership” (TCO), för att beräkna den totala ägandekostnaden.

2.2.1 Avkastning på investering (ROI)

ROI användes som beräkningsmodell för att jämföra investeringar i teknologi. ROI är designat för att ge svar på frågan: Vilket alternativ ger mest valuta för pengarna? Ett exempel på när ROI kan användas är för ett företag som skall bestämma huruvida de skall utveckla en egen lösning eller köpa en kommersiell lösning (Bojanc & Jerman-Blažič, 2008). Bojanc & Jerman-Blažič (2008) menar att ROI definierar hur mycket organisationer får av de investerade pengarna, vilket anges i procent av den returnerade investeringen över en viss tidsperiod. Formeln för ROI ser ut på följande sätt (Bojanc & Jerman-Blažič, 2008):

$$ROI = \frac{(Vinst - kostnadFörInvestering)}{kostnadFörInvestering}$$

För investeringar inom säkerhet finns en särskild beräkningsmodell som kallas return on security investment (ROSI). UcedaVelez (2008) hävdar att ROSI tillhandahåller en snabb och objektiv analys av det tillhörande värdet för en investering inom säkerhet. Enligt UcedaVelez kan en analys med ROSI underlätta i bestämmandet av huruvida investeringen i en viss säkerhetskontroll är mindre än förlusten av en utnyttjad svaghet i säkerheten. En enkel formel för ROSI ser ut på följande sätt (Bojanc & Jerman-Blažič, 2008):

$$ROSI = \frac{(ALEmedInvestering - ALEu\tan Investering - kostnadFörInvestering)}{kostnadFörInvestering}$$

ALE står för den årliga förväntade försluten. Det som står som vinst i beräkningsmodellen för ROI har alltså i ROSI bytts ut mot den förlust som görs med investering minus den förlust som görs utan investering (Bojanc & Jerman-Blažič, 2008).

2.2.2 ”Net present value” (NPV)

En väletablerad rationell ekonomisk process, som används för att budgetera vid investeringar, tillämpar kostnadseffektiv analys genom att använda NPV. Processen består av att beräkna samt jämföra det riskjusterade avdragna värdet av de förväntade vinsterna med de förväntade kostnaderna (Gordon & Loeb, 2006). Enligt Bojanc & Jerman-Blažič (2008) är NPV användbart när flera alternativ skall utvärderas. Bojanc & Jerman-Blažič ger ett enklare beräkningsexempel där en organisation väljer mellan två säkerhetslösningar. Den ena lösningen kostar 15 000 i förväg medan den andra lösningen kostar 5000 per år i tre år. Båda lösningarna kostar 15 000, men den andra lösningen är bättre då de återstående pengarna kan investeras i andra områden under en viss tid. Därför blir kostnaderna för den andra lösningen lägre än 15 000.

Enligt Bojanc & Jerman-Blažič används NPV tillsammans med ROI vid beräkningar för långsiktiga investeringar. Bojanc & Jerman-Blažič menar att ett positivt NPV innebär att projektet ger en vinst medan ett negativt värde innebär en förlust. Därav går det att säga att ett projekt är lönsamt om NPV är högre än noll.

2.2.3 “Internal rate of return” (IRR)

För att analysera stora, långsiktiga investeringar används ofta IRR, särskilt när kostnaderna ändras radikalt från ett år till nästa år. Beräkningen av IRR sker med hjälp av ett kassaflöde. IRR är sedan graden av procent där ”discount rate” skall appliceras på ett sätt att vinsterna får ett NPV som är noll (Bojanc & Jerman-Blažič, 2008).

2.2.4 Total ägandekostnad (TCO)

Modellen för TCO har tagits fram av Gartner gruppen. Med hjälp av TCO går det att analysera kostnader med att använda samt äga hårdvara och mjukvara. TCO är den totala kostnaden för en datortillgång från det att datortillgången införskaffades till att den avvecklas. Anledningen till att använda TCO är att identifiera, kvantifiera samt slutligen minska de sammanlagda kostnaderna som hör till ägandet av nätverkstillgångar (Lei & Rawles, 2003).

TCO kan delas in i två huvudsakliga kostnadsfaktorer: anskaffningskostnader samt administrativa kostnader. I en undersökning av Gartner gruppen framkom det att anskaffningskostnaderna bara utgör 20 % av TCO. Resterande del av TCO står de administrativa kostnaderna för. Exempel på anskaffningskostnader är hårdvara samt mjukvara. Exempel på administrativa kostnader är support samt installation (David, et al., 2002).

2.2.5 Svagheter och nackdelar i ROI, NPV samt IRR

ROI får utstå en del kritik. Enligt Loeb (2002) är ROI inte tillräcklig för att utvärdera beslut om investeringar. Loeb menar att ROI inte skall användas då ROI inte ger en verklig grad av vinsten. I stället hävdar Loeb att IRR skall användas för att utvärdera investeringar. Bojanc & Jerman-Blažič (2008) anser att alla tre av ROI, NPV samt IRR har både fördelar och nackdelar. För ROI är en svårighet att definiera omfattningen av investeringen. NPV och IRR har å andra sidan svårt att räkna ut ALE. Enligt Bojanc & Jerman-Blažič är NPV och IRR allt som oftast bättre än en enkel uträkning med ROI. Bojanc & Jerman-Blažič hävdar att alla tre beräkningsmodellerna bör användas för att ge den bästa bilden av en planerad investering.

Den version av ROI som används vid beräkningar för investeringar i säkerhet, ROSI, anses också ha svagheter. Davis (2005) tar upp tre problem med ROSI. Det första problemet är omognaden av konceptet samt att ROSI inte är särskilt välanvänt. Det andra problemet är att ROSI är svårt att utnyttja och att det är svårt att veta när ROSI skall användas om klara riktlinjer saknas. Det tredje problemet är att ROSI är svårt att göra beräkningar med eftersom ROSI är inkonsekvent samt använder komplexa beräkningsmetoder.

2.3 Relaterade arbeten

Av de tre rapporter som tas upp här är dem två första av Wei, et al. (2001) och Iheagwara (2004) särskilt inriktade på IDS och kostnader. Den tredje och sista rapporten av Gordon & Loeb (2002) är mer generell och berör kostnader för informationssäkerhet. Den är dock väldigt relevant då den bland annat tar upp hur mycket som skall spenderas på säkerhet.

Wei, et al. (2001) presenterar i artikeln ” Cost-Benefit Analysis for Network Intrusion Detection Systems” en metod för kostnadsfördelaktig analys samt konstruktionen av en beräkningsmodell, som baseras på kostnadsfaktorer och kategorier av olika intrång. Med hjälp av modellen skall kostnader för att upptäcka samt svara på ett intrång kunna beräknas. Enligt Wei mfl är målet att använda modellen i ett realtids IDS. Artikeln tar också upp en del om riskanalys. Bland annat står där om att beräkna värdet för tillgångar i nätverks samt hur ALE beräknas.

I artikeln “The effect of intrusion detection management methods on the return on investment” undersöker Iheagwara (2004) hur metoder för implementation, metoder

för handhavande samt policys för IDS påverkar ROI. Med artikeln strävar Iheagwara efter att visa värdet på IDS som har en väl genomtänkt implementering och effektivt handhavande. Artikeln innehåller bland annat ett ”case study” där ROI beräknas för ett IDS i ett fiktivt företag. Iheagwara introducerar också Cascading Threat Multiplier, vilken skall ge mer tyngd åt beräkningen av ALE.

Gordon & Loeb (2002) presenterar i artikeln “The Economics of InformationSecurity Investment”, en modell som avgör den optimala summan pengar som bör spenderas för att skydda ett givet set information. Gordon & Loeb skriver bland annat att det inte är nödvändigt för företag att fokusera investeringar på information med högst sårbarhet. Detta eftersom information med väldigt hög sårbarhet kan vara extremt dyr att skydda, vilket enligt Gordon & Loeb kan göra att företag hellre borde fokusera sina satsningar på information med lägre sårbarhet. Gordon & Loeb visar även en analys av två olika fall av säkerhetsintrång, där den optimala summan att spendera på säkerhet aldrig överstiger 37 % av förlusten för säkerhetsintrånget.

3 Problemprecisering

Detta avsnitt ger en enklare bakgrund till problemet samt ställer upp huvudfrågeställningen för det problem som skall lösas.

3.1 Bakgrund

Internet och lokala nätverk har de senaste åren vuxit ordentligt. Med detta har även tjänsterna som erbjuds och användarnas rörlighet ändrats på ett sätt som gör dem mer sårbara för olika typer av attacker (Bankovic´, et al., 2007). Ett antal olika verktyg finns att tillgå för att skydda företaget eller organisationen mot attacker. Antivirusprogram, brandväggar och kryptering av meddelanden är alla exempel på sådana verktyg. Trots alla verktyg som finns att tillgå är det ändå omöjligt att ha ett helt säkert system (Bankovic´ et al., 2007). På grund av det håller intrångsdetektering på att bli en allt viktigare teknik för att övervaka trafik i ett nätverk samt upptäcka intrång, som t ex otillåten nätverksaccess, eller attacker mot datorsystem (Bankovic´ et al., 2007).

Till säkerhet, och därmed IDS, hör även aspekten av kostnader. Kostnader är idag en mycket viktig aspekt som de allra flesta företag vill hålla nere. Det gäller även kostnader för informationssäkerhet. Forskare har dock upptäckt att många brister i information samt nätverk beror på besluten om ekonomi och kostnader (Fumey-Nassah, 2007). En sådan upptäckt skulle dels kunna tolkas som att det finns svårigheter kring kostnadsberäkningar som gör att brister uppstår, och dels som att ekonomi och kostnader bör tas på största allvar då de påverkar informationssäkerheten.

3.2 Frågeställning

Denna rapport syftar till att beröra både säkerhet och kostnader. Syftet med rapporten är att ur ett inköpsperspektiv visa hur kostnaderna beräknas för ett företag som vill införskaffa ett IDS. Rapporten skall även visa hur ett företag kan ta reda på lönsamheten i att införskaffa ett IDS. Meningen är också att den information som presenteras i rapporten skall leda fram till implementeringen av ett interaktivt verktyg. Verktyget skall implementeras med ett väl motiverat tillvägagångssätt för hur kostnader kring IDS beräknas. Tanken är att verktyget skall kunna användas för att beräkna kostnaderna för införskaffande av IDS samt även visa vad det kostar att inte införskaffa ett IDS.

Ytterligare ett syfte med rapporten är att reda ut omständigheter kring kostnadsberäkningarna. Meningen är alltså att rapporten även skall reflektera över faktorer som påverkar beräkningarna för kostnaderna, och där med faktorer som påverkar lönsamheten. Till det hör också att reda ut huruvida det finns faktorer som måste tas i särskild beaktning just vid investeringar i IDS.

Huvudfrågeställningen för rapporten lyder: Hur kan ett mindre eller medelstort företag beräkna lönsamheten i att investera i IDS eller i att avstå, och när blir det lönsamt att införskaffa ett IDS?

Med huvudfrågeställningen är det meningen att dessa delmål skall uppfyllas:

- Påvisa tillvägagångssätt som kan användas för att beräkna vad det kostar samt vad det inte kostar att införskaffa ett IDS, och hur tillvägagångssätten används.

- Omständigheter kring beräkningen av lönsamheten skall tas i beaktning. T ex om det finns några svårigheter runt beräkningarna, eller andra faktorer som påverkar dem.
- Ett interaktivt verktyg skall implementeras. Med det interaktiva verktyget är det meningen att en användare skall kunna göra ekonomisk bedömning för införskaffande av IDS.

Att undersöka ovan nämnda problem är viktigt ur båda de aspekter som nämnts ovan, intrångsdetektering samt kostnader. Som avsnitt 2.1 har berört är IDS ett verktyg som kan användas för att skydda nätverk och datorsystem. Tas det också i beaktande att intrångsdetektering blir en allt viktigare teknik är det både viktigt och intressant att undersöka kostnader för inköp och ägande av IDS. Detta avsnitt har även nämnt att beslut om kostnader och ekonomi i längden påverkar nätverken samt informationen. Därför är det viktigt att undersöka vilka kostnader som finns och hur de beräknas för inköp samt ägande av IDS. Det är också viktigt att undersöka omständigheterna kring beräkningen av lönsamheten. Detta då det gäller att få fram eventuella svårigheter i att bedöma lönsamheten för investering i IDS, och att för att visa om det finns aspekter som måste tas i beaktning just för investeringar i IDS. Ytterligare en viktig del när det gäller kostnaderna är att undersöka vad det kostar att inte införskaffa ett IDS.

Inköpsperspektivet har använts för att leda fram till problemen. Från synvinkeln för den eller de personer som skall införskaffa ett IDS behövs ett tillvägagångssätt för att beräkna kostnaderna, och dessutom behövs ”brytpunkten” för när företaget tjänar på att införskaffa ett IDS. En tänkbar situation ur inköpsperspektivet är att den säkerhetsansvarige på ett företag får i uppdrag att utvärdera införskaffandet av IDS. Den säkerhetsansvarige skall kunna visa om företaget behöver ett IDS eller inte. Om ett IDS behövs skall den säkerhetsansvarige kunna uppvisa vad ett IDS kostar att införskaffa samt vad det kostar att äga. Det är också viktigt att den säkerhetsansvarige kan uppvisa vad det kostar att inte införskaffa ett IDS.

Det ekonomiska inköpsperspektivet till trots bör rapporten också ses med datavetenskapliga ögon. Detta då rapporten bland annat skall presentera ett interaktivt verktyg, vilket skall automatisera processen med att göra ekonomiska bedömningar för investeringar i IDS. I detta arbete står dessutom säkerhet i fokus i och med att det är investeringar i IDS som skall undersökas. Säkerhet bör ses som datavetenskap, och i detta arbete skall säkerhet och ekonomi gå hand i hand. Det vill säga att ekonomin kan påverka säkerheten och säkerheten kan påverka ekonomin. Det är därför viktigt att kunna finna tillvägagångssätt för att bedöma investeringar i IDS då tillvägagångssätten har en möjlighet att påverka säkerheten.

4 Metod

I detta avsnitt ges en förklaring till metoden som skall användas i arbetet med rapporten. Planen för rapporten är att låta den bygga på en litteraturstudie, där de specificerade frågeställningarna i avsnitt 3 besvaras. För att höja kvaliteten i rapporten skall huvudsakligen vetenskapliga artiklar användas i litteraturstudien. Litteraturstudien kompletteras med en intervju.

4.1 Litteratursökning

De allra flesta artiklarna till litteraturstudien har påträffats via databaser, vilka finns att tillgå på Högskolan i Skövdes hemsida. De två databaser som framförallt har använts är Elin@Skövde samt ACM Portal. Dessa databaser har indirekt gjort det möjligt att söka i olika journaler och vetenskapliga tidsskrifter för datavetenskap. I databasernas sökfunktioner har ord som ”intrusion detection system”, ”cost” och ”investment” varit de mest använda. Orden har även kombinerats vid sökningar. Enligt Berndtsson, et al. (2008) är sökning i journaler samt databaser ett sätt att försäkra att källorna är relevanta.

En telefonintervju skall också genomföras. Respondenten har mångårig erfarenhet av IT-säkerhet och jobbar just nu på Ekelöw InfoSecurity AB. Metoden som skall användas för intervjun är en så kallad fokuserad intervju (Bell, 2000). Bell menar att det är viktigt att lämna viss frihet för respondenten. På så sätt kan respondenten utveckla det som är viktigt. Bell hävdar också att en viss struktur i intervjun är viktig, vilket enligt Bell ger en viss garanti för att alla ämnesområden kommer med. Den fokuserade intervjun uppfyller dessa mål. Inget frågeformulär används. Dock ges en struktur genom att utvalda teman täcks under intervjuns gång. Frågor ställs, men utrymme ges också åt respondenten att prata omkring de ställda frågorna (Bell, 2000). Observera att i intervjun till denna rapport skall ett frågeformulär användas, dock skall frågorna vara öppna vilket ger frihet till respondenten samt att respondenten får möjlighet att utveckla och prata kring frågorna.

4.2 Interaktiva verktyg

Implementeringen av interaktiva verktyg har skett i Microsoft Excel. Metoden har varit att använda information från resultatet. Utifrån informationen har sedan verktygen skapats som kalkylblad i Excel där kriterier från resultatet har förts över till kalkylbladen.

4.3 Metodval

Anledningen till att en litteraturstudie skall användas är att den är relativt enkel att genomföra, och att informationen från den bör ses som relevant. Detta då informationen i första hand skall baseras på vetenskapliga artiklar samt böcker, vilket i sin tur leder till ett trovärdigt resultat. Syftet med litteraturstudien är att på vetenskapliga grunder besvara huvudfrågeställningen samt uppfylla delmålen.

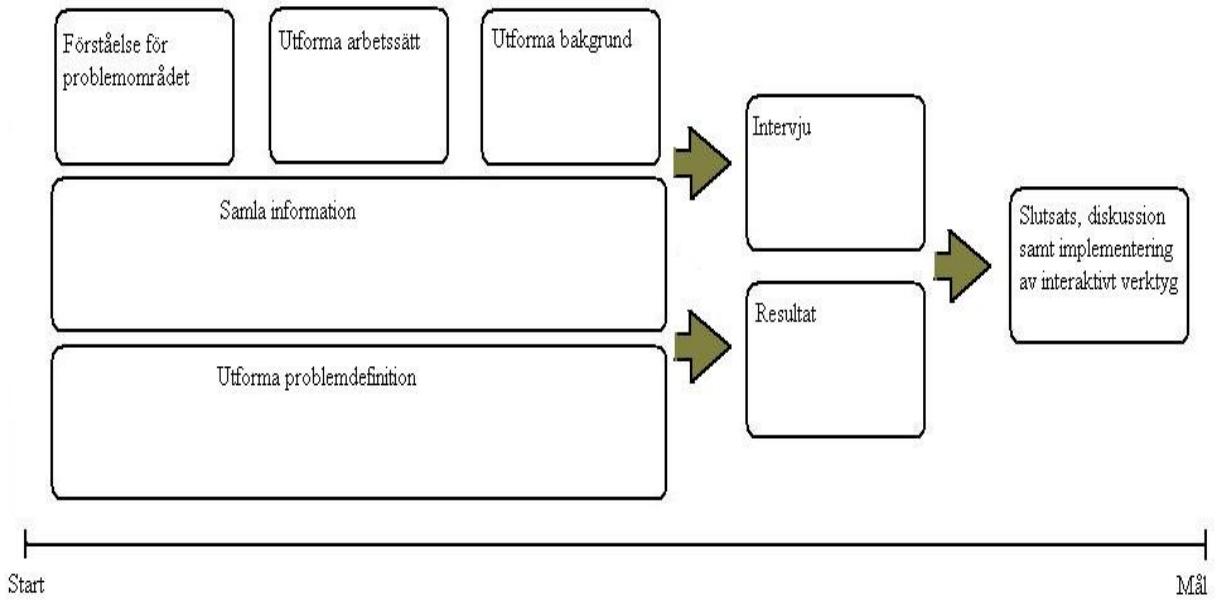
Intervjun som skall genomföras skall inte användas för att besvara huvudfrågeställningen eller uppfylla delmålen. Syftet med intervjun är att stärka och utöka diskussionen samt slutsatserna.

Valet av metod bör betraktas som att det finns empiriskt stöd för teorin, där problemet skall lösas via en litteraturstudie och där en extra dimension skall ges via intervjun. Detta gör att framförallt litteraturstudien relaterar på ett bra sätt till problemet.

Metoden diskuteras i avsnitt 7.1 där bland annat ett alternativ till den valda metoden tas upp.

5 Tillvägagångssätt

Tillvägagångssättet kan beskrivas som ett stegvist utförande där ett steg har lett fram till nästa steg. I stora drag har ett problem definierats, information samlats in enligt metoderna beskriva i avsnitt 4, utifrån den insamlade informationen har ett resultat presenterats och diskuterats. Stegen i tillvägagångssättet kan beskrivas med följande figur:



Figur 1- Bild över hur arbetet har utförts

Genom att titta på figur 1 går det att urskilja att arbetet har skett i tre steg. I ett första steg så har information samlats in. Det har skett parallellt med att problemområdet har undersökts, ett arbetssätt har definierats och att bakgrunden har utformats. Under hela detta steg har också problemet definierats. Problemet har under detta steg gått från att vara tämligen diffust och omfattande till att bli tydligt och detaljerat.

Det andra steget har utformats via utförandet i första steget. Utifrån bakgrund, insamlad information samt det utformade problemet har resultat och intervju utarbetats. Arbetet med resultatet och intervjun har delvis utförts parallellt, där frågor till intervjun har tagits fram utmed att resultatet färdigställts. Slutligen har intervjun genomförts.

I det tredje och avslutande steget har slutsats och diskussion sammanställts samt att två enklare interaktiva verktyg har implementerats. Diskussion och slutsats baseras framförallt på den information som tagits fram i resultatet, men både i slutsats och i synnerhet i diskussionen har också intervjun använts. De interaktiva verktygen har utarbetats i Microsoft Excel, och de baseras helt och hållet på informationen i resultatet.

6 Resultat

I detta avsnitt beskrivs i första hand de tre beräkningsmodellerna ROSI, NPV samt IRR. Varje modell förklaras, en enklare förklaring till datainsamling ges, och till varje modell ges också ett beräkningsexempel. Avsnittet innehåller även en enkel förklaring till kostnadsmodeller samt kostnadseffektivitet för IDS.

Det finns framförallt en anledning till att fokusen i detta avsnitt ligger på dessa beräkningsmodeller. Anledningen är att ROSI (eller ROI), NPV samt IRR är relativt välanvända. Som avsnitt 2.2 redan beskrivit är det (av 408 svarande) 44 % som använder ROI, 26 % som använder NPV samt 23 % som använder IRR. En annan anledning skulle kunna vara att beräkningsmodellerna i sig är relativt enkla att använda. Dock kan värdena som sätts in i modellerna (se avsnitt 6.4) vara desto svårare att hantera, vilket diskuteras i avsnitt 8.

6.1 ROSI

Organisationer som vill ta reda på värdet av ett IDS innan de installerar det är enligt Iheagwara (2004) beroende av ett positivt ROI för att kunna besluta om de ska investera i ett IDS. Iheagwara menar att ett positivt ROI kan bli begripligt genom att analysera skillnaden mellan ALE utan IDS samt ALE med IDS, anpassat för tekniska och handhavandekostnader. Även Bojanc & Jerman-Blažič (2008) hävdar att vinsten kan förklaras genom skillnaden mellan ALE utan någon säkerhetsinvestering och ALE med säkerhetsinvestering. Bojanc & Jerman-Blažič presenterar en enkel formel för ROSI (samma formel som återfinns i avsnitt 2.2.1), och även en enkel formel för vinsten:

$$ROSI = \frac{(ALEuSi - ALEmSi - investeringskostnaden)}{investeringskostnaden}$$

$$\text{Vinsten} = \text{ALEuSi} - \text{ALEmSi}$$

ALEuSi är ALE utan säkerhetsinvestering och ALEmSi är ALE med säkerhetsinvestering.

För att kunna utföra beräkningar med ovanstående formler krävs det att ALE kan beräknas för enskilda händelser. Bojanc & Jerman-Blažič ger följande formler för att beräkna ALE:

$$\text{SLE} = \text{AV} * \text{EF}, \text{ och } \text{ALE} = \text{SLE} * \text{ARO}$$

SLE är ”single loss exposure” och representerar den totala summan av intäkten som förloras vid en enskild förekomst av en viss risk. Det vill säga att SLE är den valutasumma som hör ihop med en viss enskild händelse, vilken är den möjliga förlust en organisation kan göra om ett specifikt hot utnyttjar en sårbarhet (Bojanc & Jerman-Blažič, 2008). SLE beräknas alltså genom att multiplicera valutavärdet av en tillgång (AV) med exponeringsfaktorn (EF). EF representerar i procent hur mycket ett realiserat hot skulle kunna ge i förlust för en viss tillgång (Bojanc & Jerman-Blažič, 2008). ARO är den årliga graden av förekomst, vilket innebär det antalet gånger under ett år som en organisation förväntar sig att en viss risk skall ske.

ALE beräknas slutligen genom att multiplicera SLE med ARO. Resultatet representerar den totala summa i pengar som en organisation kan förlora under ett år om inget görs för att minska risken (Bojanc & Jerman-Blažič, 2008). Den totala

ALE:n för en organisation beräknas genom att addera ALE:s för alla händelser (Wei m.fl. 2001).

6.2 NPV

NPV kan användas för att göra beräkningar på investeringar i säkerhet. Ett nuvärde beräknas genom att alla framtida inbetalningsöverskott diskonteras med hjälp av en vald kalkylränta (Lönnqvist, 2005). Enligt Lönnqvist avgörs en investerings lönsamhet av om nuvärdet av inbetalningsöverskotten överstiger investeringens storlek, eller som Lönnqvist (2005, s. 221) själv uttrycker det: ”En investering är lönsam om den har ett nuvärde som är större än noll.”

Formeln för NPV kan uttryckas på följande sätt (Lönnqvist, 2005):

$$investeringensNuvärde = \frac{a1}{(1+k)^1} + \frac{a2}{(1+k)^2} + ... + \frac{aN}{(1+k)^n} + \frac{R}{(1+k)^n} - G$$

Där aN är inbetalningsöverskott år N,

k är kalkylräntan,

G är grundinvesteringen,

R är restvärdet,

och n är ekonomisk livslängd.

6.3 IRR

Med hjälp av IRR kan den årliga avkastningen som en investering väntas ge beräknas. En investering blir mer och mer lönsam i takt med att IRR stiger, och kriteriet för att en investering skall vara lönsam är att värdet för IRR är lika med eller större än kalkylräntan (Lönnqvist, 2005).

Lönnqvist (2005) presenterar en metod för IRR där användaren av metoden får pröva sig fram. Enligt Lönnqvist borde ett investeringsprojekt som ger precis vad som krävs ha ett värde för IRR som är lika stort som värdet för kalkylräntan. Detta grundar Lönnqvist på att kalkylräntan är kravet på avkastning medan IIR är den avkastning ett investeringsprojekt faktiskt beräknas ge. Lönnqvist menar att en investering med lika stora värden på kalkylräntan och IRR borde ge ett nuvärde på noll kronor, och utifrån det hävdar Lönnqvist att det går att finna värdet för IRR genom att hitta den räntesats som ger nuvärdet noll.

Formeln för IRR kan uttryckas på följande sätt (Lönnqvist, 2005):

$$0 = \frac{a1}{(1+IRR)^1} + \frac{a2}{(1+IRR)^2} + ... + \frac{aN}{(1+IRR)^n} - G$$

Där 0 är NPV (nuvärdet),

aN är inbetalningsöverskott år N,

IRR är det eftersökta värdet på den interna räntan,

G är grundinvesteringen,

och n är ekonomisk livslängd.

6.4 Datainsamling

En viktig del för företag och organisationer, som skall använda någon eller några av beräkningsmodellerna i avsnitten innan, är vetskapen om hur indata till modellerna tas fram. För ROSI är ALEuSi en av de första parametrarna att beräknas (se avsnitt 6.1). För att ta fram ALEuSi krävs det att företaget kan utföra en riskanalys, vilken exempelvis kan delas in i fyra steg (Wei, et al., 2001):

1. Identifiera vilka tillgångar som finns samt ge dem valutavärden. För IDS gäller det alltså att uppskatta och värdera de tillgångar som kan skyddas av IDS. En sådan tillgång kan t ex vara en server. I beräkningen av ALEuSi är det AV som representerar tillgångens värde

2. Identifiera hot och sårbarheter. När alla tillgångar är värderade och identifierade skall hoten mot dessa tillgångar identifieras. Ett exempel på ett hot som IDS kan skydda mot är otillåten access. Efter att hoten blivit identifierade måste sårbarheterna som hoten kan utnyttja identifieras.

   När hoten och sårbarheterna har identifierats går det att beräkna den förlust som uppstår om ett hot utnyttjar en sårbarhet. T ex om en obehörig person får otillåten access, då måste den möjliga förlusten för en sådan händelse beräknas. I beräkningen av ALEuSi är det SLE som representerar denna beräkning, och som avsnitt 6.1 beskriver beräknas SLE genom att multiplicera AV med EF. EF måste uppskattas för varje hot och tillgång. Ett företag kan uppskatta att om en server utsätts för virus innebär det en förlust på 35 % av serverns värde. Samma företag kan t ex också uppskatta att en server som utsätts otillåten access får en förlust på 50 % av värdet.

3. Beräkna försluten, alltså ALE. Som avsnitt 6.1 beskriver kan ALE beräknas genom att multiplicera SLE med ARO, och kommer alltså gälla varje enskild händelse. ARO är indata som återigen måste uppskattas. Olika hot kan realiseras olika antal gånger under en viss tid. Ett företag kan uppskatta att en server blir angripen av virus fyra gånger per ett år, medan företaget kan uppskatta att serverrummet utsätts för brand vart fjärde år. Eftersom ALE gäller för varje enskild händelse måste den totala ALE:n beräknas genom att addera ihop ALE:n för alla händelser, vilket beskrivits i avsnitt 6.1. I fallet ovan skulle den totala ALE:n beräknas genom att addera ALE för virusangrep samt ALE för brand i serverrum.

4. Identifiera vilka skydd som finns samt hur mycket de kan skydda. I detta fall IDS.

ALEmSi, som är nästa parameter vid kalkylering av ROSI, kan beräknas genom att ta reda på hur effektivt IDS:et i fråga är. Som avsnitt 6.1 beskriver beräknas vinsten genom att jämföra ALEuSi med ALEmSi, i detta fall med eller utan IDS.

Den sista parametern för ROSI är investeringskostnaden, vilken kan delas upp i två delar. Dels i kostnaden för själva inköpet (det finns IDS:er som är open source, vilket i så fall tar bort denna kostnad) av IDS:et och dels kostnaden för handhavande. I handhavandekostnaden gäller det att få in alla kostnader. Exempel på sådana

kostnader kan vara lönekostnader, kostnader för att svara på alarm, kostnader för falska alarm, och så vidare.

Indata till NPV skiljer sig mot ROSI, men där finns också en del att återanvända. Precis som med ROSI behöver en riskanalys göras (se de fyra stegen här ovan). Återigen beräknas vinsten genom att jämföra ALE med och utan IDS (ALEuSi samt ALEmSi). Inbetalningsöverskottet beräknas genom att subtrahera kostnaden från vinsten, vilket beskrivs närmare i exemplet för NPV i avsnitt 6.5.2. Observera att kostnaden i detta fall är handhavandekostnaden för IDS:et i fråga. Kostnaden för inköpet (om det inte är open source) av IDS representeras av grundinvesteringen i beräkningen av NPV.

De indata som skiljer sig är kalkylräntan samt ekonomisk livslängd. Kalkylräntan används för att kunna lönsamhetsbedöma en investering där betalningar är gjorda vid olika tidpunkter. Detta eftersom betalningar som är gjorda vid olika tidpunkter är olika mycket värda, vilket gör att en räntesats behövs så att dessa betalningar kan värderas. Oftast bestäms kalkylräntan för ett företag utifrån krav som ställs av banker och ägare. Kraven kan relateras till den ränta som ett företag har på sina lån (Lönnqvist, 2005). Ett möjligt sätt att beräkna kalkylräntan är (Lönnqvist, 2005):

$$(\text{andelen lån} * \text{låneränta}) + (\text{andelen eget kapital} * \text{ägarnas avkastningskrav})$$

Den ekonomiska livslängden är den tidsperiod som en investering är lönsam under (Lönnqvist, 2005). Det gäller alltså att bestämma hur länge IDS:et i fråga skall vara i drift.

Vid beräkningar med IRR går det att återanvända (eller beräkna på nytt ifall bara IRR skall användas) ekonomisk livslängd, grundinvestering och inbetalningsöverskott från NPV. Som avsnitt 6.3 beskriver gäller det att pröva sig fram för att hitta värdet på IRR.

6.5 Exempel

I detta avsnitt följer exempel för beräkning med var och en av beräkningsmodellerna. Observera att siffrorna enbart är approximerade för att illustrera dessa exempel och har ingen förankring i verkligheten.

6.5.1 Beräkning med ROSI

Följande exempel baseras på Bojanc & Jerman-Blažič (2008) formler och beräkningar.

Företag X vill beräkna om det är lönsamt att införskaffa ett IDS till verksamheten. IDS:et kostar 20 000 kr att köpa in och kostar därutöver 40 000 kr om året i handhavandekostnader. IDS:et förväntas kunna upptäcka 80 % av alla intrång.

Företag X uppskattar att deras server kan utsättas för en virusattack samt intrång från icke behöriga individer. ALEuSi för händelserna kan beräknas av Företag X med formeln (se avsnitt 6.1):

$$ALEuSi = SLE * ARO,$$

vilken kan göras om till:

$$ALEuSi = AV * EF * ARO,$$

eftersom SLE = AV * EF (se avsnitt 6.1).

Företag X uppskattar värdet av servern till 1 000 000 kr (AV). De uppskattar att en virusattack skulle innebära 1 % förlust av serverns värde (EF) samt att en virusattack skulle ske 5 gånger på ett år (ARO). Företag X uppskattar att ett intrång skulle innebära 15 % förlust av serverns värde samt att det skulle kunna ske vart annat år. Företag X:s beräkning för attackerna ser ut på följande sätt:

$$\text{Virusattack}: 1\,000\,000 * 0.01 * 5 = 50\,000 \text{ kr}$$

$$\text{Intrång}: 1\,000\,000 * 0.15 * 0.5 = 75\,000 \text{ kr}$$

Företag X:s totala ALEuSi beräknas genom att addera 50 000 med 75 000 vilket ger 125 000 kr. Den eventuella förväntade vinsten kan beräknas av företag X med formeln (se avsnitt 6.1):

$$\text{Vinsten} = \text{ALEuSi} - \text{ALEmSi},$$

vilken kan göras om till:

$$\text{Vinsten} = \text{ALEuSi} * \text{IDS}: \text{ets effektivitet} \rightarrow 125\,000 * 0.80 = 100\,000 \text{ kr}$$

Vinsten blir alltså 100 000 kr. Företag X beräknar ROSI enligt följande formel (se avsnitt 6.1):

$$ROSI = \frac{(ALEuSi - ALEmSi - investeringskostnaden)}{investeringskostnaden},$$

vilken kan göras om till:

$$ROSI = \frac{(ALEuSi * IDS: etsEffektivitet) - investeringskostnaden}{investeringskostnaden},$$

där det som står inom parentesen är vinsten och ger i detta fall:

$$\frac{(100\,000 - 20\,000 - 40\,000)}{(20\,000 + 40\,000)} = 0.66$$

Företag X kommer alltså få ett positivt värde på ROSI som är 66 %. Observera att beräkningen är gjord för ett år och med antagandet att kostnaden för IDS:et (20 000 kr) betalas under det året.

6.5.2 Beräkning med NPV

Samma värden som används i exemplet i avsnitt 6.5.1 används även i detta exempel. Exemplet baseras på Lönnqvists (2005) samt Bojanc & Jerman-Blažič (2008) formler och beräkningar.

Företag X vill beräkna om det är lönsamt att införskaffa ett IDS till verksamheten genom att beräkna nuvärdet för investeringen. Den ekonomiska livslängden för IDS:et uppskattar företag X till tre år. Företag X bestämmer också att en kalkylränta på 5 % skall användas. Inbetalningsöverskottet kan uppskattas genom vinsten minus kostnaderna:

$$\text{Vinsten} = \text{ALEuSi} * \text{IDS}: \text{ets effektivitet} \Rightarrow 125\,000 * 0.80 = 100\,000 \text{ kr}$$

Från vinsten dras sedan kostnaderna vilket är 40 000 kr, alltså 100 000 – 40 000, som då ger ett inbetalningsöverskott på 60 000 kr (vilket i detta exempel kommer gälla per år för alla tre åren). Företag X har sedan alla värden som behövs och kan sätta in dem i formeln för NPV (se avsnitt 6.2), vilket ger följande:

$$nuvär\,\det = \frac{60\,000}{(1+0.05)^1} + \frac{60\,000}{(1+0.05)^2} + \frac{60\,000}{(1+0.05)^3} - 20\,000$$

Resultatet blir 143 395 kr. Investeringen i ett IDS för företag X är alltså enligt beräkningen med NPV lönsam.

6.5.3 Beräkning med IRR

Samma värden som används i exemplen i avsnitt 6.5.1 samt .6.5.2 används även i detta exempel. Exemplet baseras på Lönnqvists (2005) formel.

Företag X vill beräkna lönsamheten i investeringen i ett IDS med hjälp av metoden för IRR. Sätter företag X in alla värden (även värdet för inbetalningsöverskottet från avsnitt 6.5.2) i formeln för IRR (se avsnitt 6.3) ser det ut på följande vis:

$$0 = \frac{60\,000}{(1+IRR)^1} + \frac{60\,000}{(1+IRR)^2} + \frac{60\,000}{(1+IRR)^3} - 20\,000$$

Härifrån får företag X pröva sig fram för att hitta det värde på IRR som ger ett nuvärde som ligger så nära 0 det är möjligt. I den beräkning som görs här blir resultatet 295 %.

6.5.4 Sammanfattning

En sammanfattning av beräkningarna för företag X ger följande tabell (1):

Investering beräknad med ROSI (år 1):	66 %
Investering beräknad med NPV:	143 396 kr
Investering beräknad med IRR:	295 %

Tabell 1

Det kan vara värt att notera hur siffrorna påverkar beräkningarna. Antag att företag X beräknar handhavandekostnaden till 60 000 kr istället för 40 000 kr. Tabellen (2) skulle då ändras och se ut på följande vis:

Investering beräknad med ROSI (år 1):	25 %
Investering beräknad med NPV:	88 930 kr
Investering beräknad med IRR:	192 %

Tabell 2

Noterbart kan också vara att beräkningen med ROSI gäller för år ett där det förutsätts att IDS:et betalas under det året. Om värdet för ROSI beräknas för år två skulle ROSI i tabell 1 få värdet av 150 %, och i tabell 2 skulle värdet för ROSI bli 66 %.

6.6 Kostnadseffektivitet samt kostnadsmodeller

En viktig aspekt för ett IDS är att IDS:et skall vara kostnadseffektivt. IDS:et skall helt enkelt inte kosta mer än vad den förväntade förlusten beräknas göra. IDS:et behöver därför överväga ”trade-offs” mellan kostnadsfaktorer, vilka minst bör inkludera kostnader för utveckling, kostnader för skador som uppstår på grund av intrång,

kostnaderna av att svara på intrång samt kostnader för användandet (Iheagwara, 2004). Lee, et al. (2002) menar att för att kunna konstruera kostnadskänslig intrångsdetekteringsmodeller måste det finnas en förståelse för kostnadsfaktorerna samt hur de skall definieras. Enligt Lee, et al. är följande faktorer de huvudsakliga kostnadsfaktorerna som hör ihop med intrångsdetektering: kostnad för skada (skadekostnad), kostnad för att svara (svarskostnad) samt kostnad för användande (användarkostnad). Skadekostnad beror framförallt på värdet av det attackerade målet samt hur stor skada som kan orsakas av attacken. T ex skulle det vara en större skadekostnad för en attack som ger angriparen tillgång till root än om angriparen får tillgång till lokala användare. Svarskostnaden beror oftast på vilken typ av svarsmekanism som används. Svarsmekanismer kan t ex bero på vilken typ av attack det är och vilken resurs som blir attackerad. Svar kan vara automatiserade eller manuella, där manuella svar har en högre svarskostnad än automatiserade svar. Den huvudsakliga kostnaden för ett IDS står användarkostnaden för. Användarkostnaden innefattar all den tid samt alla de resurser som krävs för att hantera den övervakade dataströmmen (Lee, et al., 2002).

Genom att använda skadekostnad, svarskostnad samt användarkostnad går det att skapa följande kostnadsmodell för riskanalysberäkningar:

$$totalKostnad(e) = \sum^{N} (betydandekostnad + användarkostnad(e)),$$

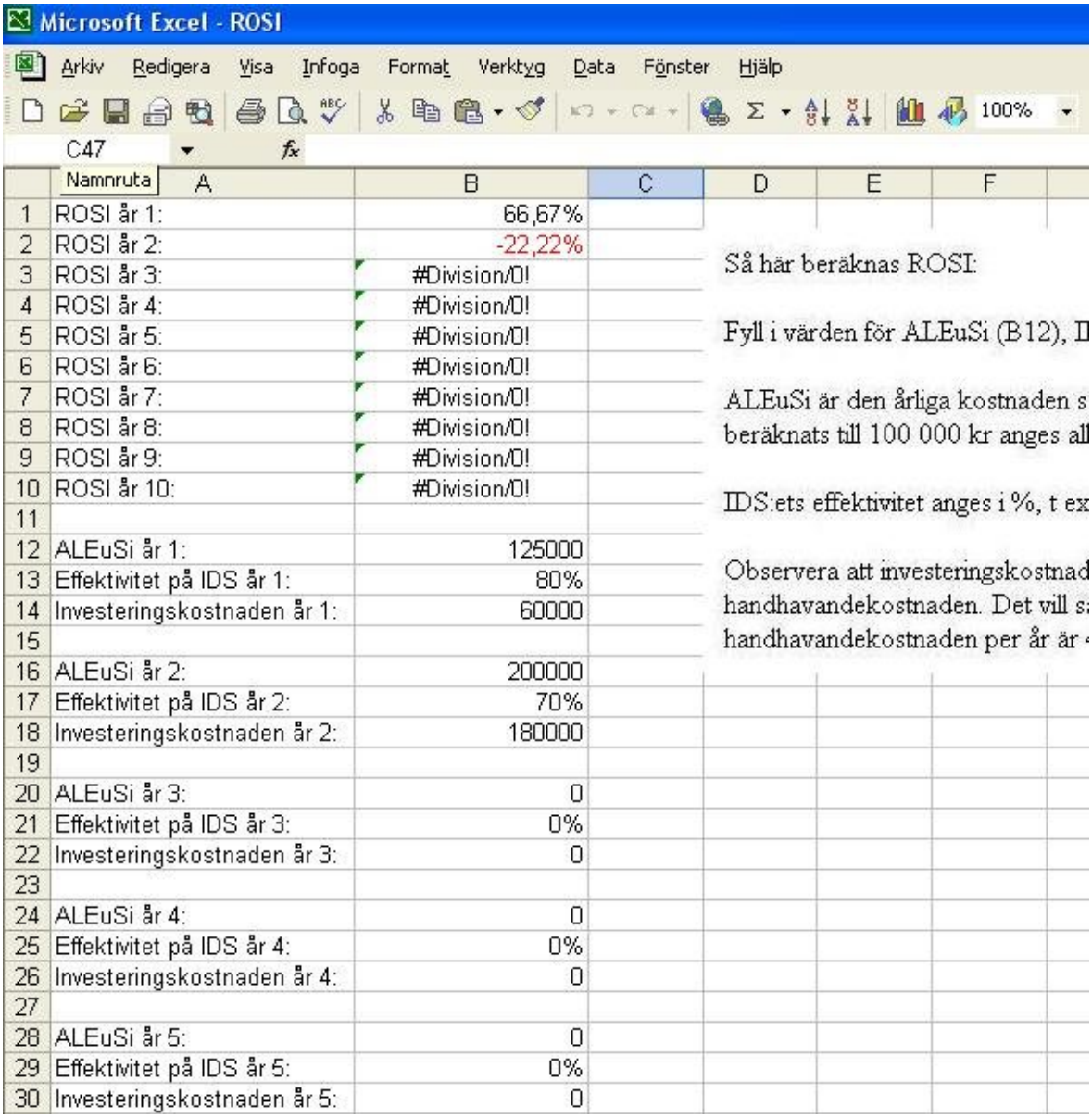
där den totala kostnaden gäller för en viss händelse e, och N är händelsenumret. Betydandekostnad är kostnaden av den förutsägelse som IDS:et gör för en viss intrångsklassificerad händelse e, vilken bestäms av svarskostnaden samt skadekostnaden (Iheagwara, et al., 2004).

I en annan kostnadsmodell används fem olika förutsägelser. Dessa är Falska Negativa (FN), Sanna Positiva (SP), Falska Positiva (FP), Sanna Negativa (SN) samt oklassificerade träffar. Förutsägelserna kan sedan användas för att bestämma kostnader. FN är t ex den kostnad när en attack ej upptäcks, vilket t ex kan bero på att inget IDS är installerat. Ett annat exempel är SP som innebär att en attack upptäcks, vilket ger en kostnad av att upptäcka attacken samt svara på attacken (Iheagwara, et al., 2004).

Lee, et al. (2002) menar att ett IDS skall avgöra hur det skall agera utifrån kostnaderna för att svara på en attack jämfört med skadan för attacken. T ex hävdar Lee, et al. att om kostnaden för skadan är mindre än kostnaden för att svara skall IDS:et ignorera attacken. Ett sådant agerande minskar enligt Lee, et al. den totala kostnaden för IDS:et. Enligt Lee, et al. är också en attacktaxonomi viktig för att få fram meningsfulla kostnadsmått. Taxonomin grupperar intrång på ett sätt att mått för kostnader kan göras för liknande attacker. Via olika perspektiv kan intrång kategoriseras och analyseras. Intrången kan bland annat kategoriseras efter vilken effekt de har, t ex om ”denial-of-service” utförs eller inte. Tack vare detta kan en attacktaxonomi användas för att uppskatta svarskostnader samt skadekostnader (Lee, et al., 2002).

6.7 Interaktivt verktyg

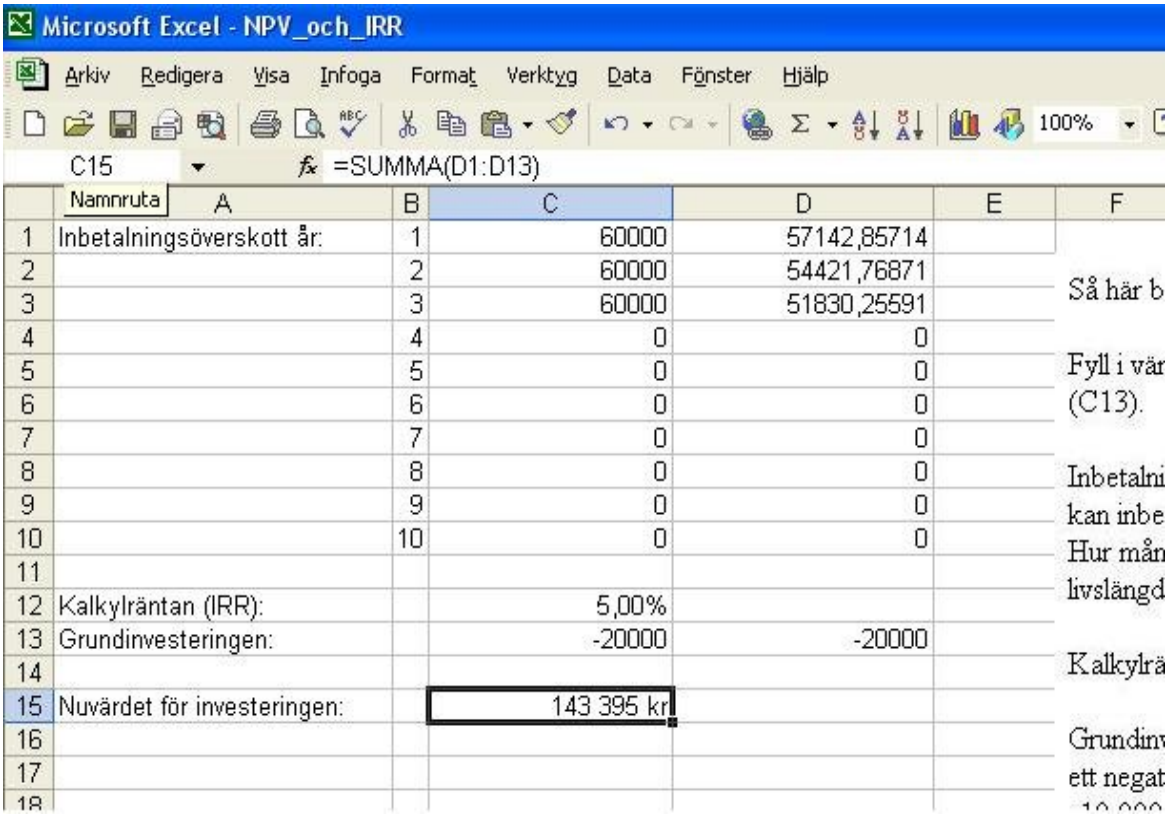
Resultaten som presenterats för ROSI, NPV samt IRR har resulterat i två enklare interaktiva verktyg i form av två kalkylblad i Microsoft Excel, vilka kan användas för att beräkna lönsamhet för investeringar i IDS. Ett kalkylblad används för att beräkna ROSI (se figur 2) och det andra används för att beräkna NPV samt IRR.



	A	B	C	D	E	F
1	ROSI år 1:	66,67%				
2	ROSI år 2:	-22,22%				
3	ROSI år 3:	#Division/0!				
4	ROSI år 4:	#Division/0!				
5	ROSI år 5:	#Division/0!				
6	ROSI år 6:	#Division/0!				
7	ROSI år 7:	#Division/0!				
8	ROSI år 8:	#Division/0!				
9	ROSI år 9:	#Division/0!				
10	ROSI år 10:	#Division/0!				
11						
12	ALEuSi år 1:	125000				
13	Effektivitet på IDS år 1:	80%				
14	Investeringskostnaden år 1:	60000				
15						
16	ALEuSi år 2:	200000				
17	Effektivitet på IDS år 2:	70%				
18	Investeringskostnaden år 2:	180000				
19						
20	ALEuSi år 3:	0				
21	Effektivitet på IDS år 3:	0%				
22	Investeringskostnaden år 3:	0				
23						
24	ALEuSi år 4:	0				
25	Effektivitet på IDS år 4:	0%				
26	Investeringskostnaden år 4:	0				
27						
28	ALEuSi år 5:	0				
29	Effektivitet på IDS år 5:	0%				
30	Investeringskostnaden år 5:	0				

Figur 2 – Bild på hur kalkylbladet för ROSI ser ut

Som figur 2 visar är det med kalkylbladet för ROSI möjligt att beräkna ROSI för tio olika år. För varje år ROSI skall beräknas anges värden för ALEuSi, IDS:ets effektivitet samt investeringskostnaden. Dessa värden måste alltså beräknas och uppskattas innan beräkningen av ROSI kan utföras (se avsnitt 6.1 samt 6.4 för närmare beskrivning av indata till ROSI). Svaret/svaren ges sedan i rutorna B1 till B10. Ett positivt svar skrivs ut med svart text medan ett negativt skrivs ut med röd text, vilket figur 2 illustrerar i rutorna B1 och B2.



Figur 3 – Bild på hur kalkylbladet för NPV och IRR ser ut

Figur 3 visar kalkylbladet för NPV och IRR, där det alltså är möjligt att göra beräkningar med båda modellerna. För att beräkna NPV behövs värden för inbetalningsöverskott, kalkylräntan samt grundinvesteringen. Det är också viktigt att veta livslängden på investeringen eftersom den avgör för hur många år som inbetalningsöverskottet skall anges (se avsnitt 6.2, 6.3 samt 6.4 för närmare beskrivning av indata till NPV och IRR). När värdena har matats in ges svaret för NPV, det vill säga investeringens nuvärde, i ruta C15.

Som redan nämnts används kalkylbladet i figur 3 också till att beräkna IRR. Värdena anges på samma sätt som vid beräkning av NPV med skillnaden att kalkylräntan skall ses som IRR. Som avsnitt 6.3 beskriver går det att finna IRR genom att finna den räntesats som ger nuvärdet noll. När IRR skall beräknas med kalkylbladet skall alltså ett värde anges i ruta C12 som resulterar i att värdet i ruta C15 blir noll, eller så nära noll som möjligt.

Precis som i kalkylbladet för ROSI presenteras positiva resultat med svart text medan negativa resultat presenteras med röd text.

7 Diskussion

I detta avsnitt diskuteras metoden som använts samt resultatet som uppnåtts.

7.1 Metod

Valet att bygga rapporten på en litteraturstudie som metod har lett fram till ett resultat med de tre beräkningsmodellerna, vilka baseras på information från artiklar och böcker. Litteraturstudien resulterade också i att rapporten tar upp datainsamlingen till beräkningsmodellerna samt de interaktiva verktygen, vilka baseras på beräkningsmodellerna. Informationen från intervjun har resulterat i att framförallt diskussionen, men också slutsatserna har stärkts utifrån respondentens svar.

Enligt Andersen & Gamdrup (1994) är en nackdel med litteraturstudier att den information som samlas in är fastslagen redan från början. Ett alternativ till att låta rapporten bygga på en litteraturstudie hade varit att använda intervjuer i större utsträckning för att samla in information. T ex hade ett antal väl standardiserade samt strukturerade frågor kunnat ställas till en mängd respondenter, kunniga inom området. Svaren hade kunnat användas för att bestämma vilka tillvägagångssätt för kostnadsberäkningar som skulle presenteras i resultatet. En litteraturstudie hade sedan kunnat genomföras för tillvägagångssätten för att visa hur de fungerar. Resultatet från en sådan metod hade troligtvis varit mer användarinriktat. Det vill säga att det troligen hade gett en bra bild för hur kostnadsberäkningar för investeringar i IDS går tillväga ute bland företagen, och vika tillvägagångssätt som faktiskt används. Tillvägagångssätten hade dock fortfarande kunnat gestaltas av de tre beräkningsmodellerna som presenteras i denna rapport.

Anledningen till att intervjuer inte har använts i större utsträckning är att tid inte har funnits till det. För att låta rapporten bygga på intervjuer hade betydligt fler än en intervju behövts genomföras.

7.2 Resultat

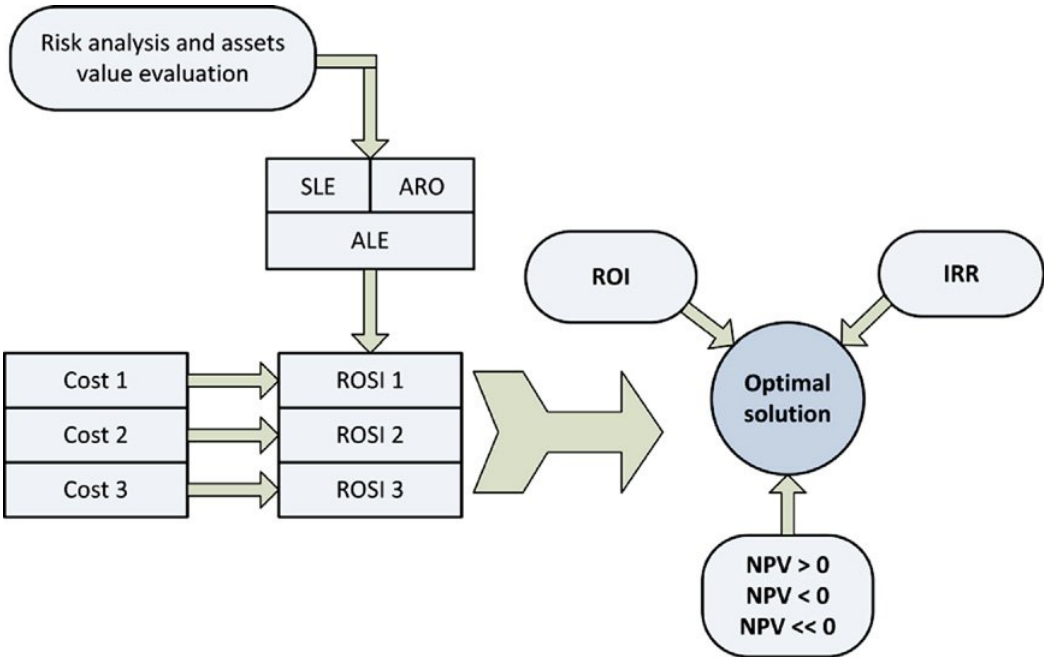
Som rapporten redan nämnt i avsnitt 6.4 är ALEuSi en av de första parametrarna att beräkna, och den används i alla tre beräkningsmodellerna (ROSI, NPV samt IRR). ALEuSi är den kanske viktigaste parametern för beräkningsmodellerna då den visar den förlust som ett företag utsätts för. Ett företag som vill investera i ett IDS måste veta vad det kostar dem att inte besitta ett IDS. Om ett företag inte vet vad kostnaden utan IDS är kan de heller inte jämföra den eventuella förtjänsten av att ha ett IDS med något.

I bland annat avsnitt 6.5.1 beskrivs det att ALEuSi kan beräknas genom att multiplicera SLE med ARO. Det är dock ingen enkel beräkning att göra. Att beräkna samt uppskatta värden för SLE och ARO är svårt. Detta eftersom det är väldigt få företag och organisationer som spårar upp samt rapporterar säkerhetsincidenter, vilket leder till att det finns väldigt lite bra data att utgå från (Bojanc & Jerman-Blažič, 2008). Ett företag som skall beräkna t ex ALE har en inte helt lätt uppgift. Hur mycket förlorar ett företag vid ett intrång? Att uppskatta de direkta förlusterna om t ex data raderas av en angripare är en sak. Men vad kostar det företaget om dataintrånget resulterar i förlorade kunder? Hur beräknar företag sådana kostnader? I intervjun tar respondenten upp samma problem: ”Och det är där det kommer, vad kommer det att kosta, vad kommer ett intrång kosta? Vad kommer det att kosta företaget i både

förlorade pengar, förlorade intäkter, att det läcker ut information om företaget, förlorade affärer eller nånting annat?".

Processen att få fram korrekta siffror till beräkningsmodellerna är det allra svåraste, och det gäller inte bara ALE, SLE och ARO utan även handhavandekostnaderna, ekonomisk livslängd och så vidare. I avsnitt 6.5.4 i rapporten påvisas skillnaden i beräkningarna för ROSI, NPV samt IRR när handhavandekostnaden ändras. Det visar det ganska självklara i att resultatet påverkas av de indata som tas fram till beräkningsmodellerna. Men det också hur viktigt det är att få fram korrekta värden för indata till beräkningsmodellerna. Alla siffror gör skillnad, även mindre förändringar kan göra att snäva beräkningar kan svänga från positiva till negativa, eller tvärtom. Detta är något som också tas upp i resultatet (se avsnitt 8) där IDS:ets effektivitet används som exempel, men det gäller som sagt all indata som skall användas. Beräkningsmodellerna är också väldigt beroende av "instabila" värden. Vet företaget i fråga om IDS:ets effektivitet verkligen är 80 %? Kan företaget vara säkra på att ett visst hot kommer inträffa två gånger per år och att det kommer kosta x antal kronor? Stämmer verkligen företagets beräkning av ALEuSi till 100 %? Svaret på dessa frågor är troligtvis nej. Det är troligtvis näst intill omöjligt att företag skall uppskatta och beräkna exakta värden som stämmer. Dock är det nödvändigt att dessa värden blir så korrekta som möjligt om resultatet skall vara tillförlitligt, vilket bör ses som en svår uppgift.

En viktig fråga är vilken eller vilka beräkningsmodeller som skall användas vid investeringar i IDS. Som avsnitt 2.2.5 redan tagit upp anser Bojanc & Jerman-Blažič (2008) att alla tre beräkningsmodellerna bör användas. Se figur 4 för det tillvägagångssätt som Bojanc & Jerman-Blažič förespråkar.



Figur 4 – Figuren visar den process som Bojanc & Jerman-Blažič förespråkar (Bojanc & Jerman-Blažič, 2008).

Minst två av beräkningsmodellerna bör i alla fall användas när en investering skall göras, förslagsvis ROSI och NPV. ROSI och NPV är enklare att förstå och dessutom är de inte lika "ekonomiska" som IRR. Det vill säga, ROSI ger ett svar i procent och NPV ger ett svar i kronor medan IRR används för att beräkna internräntan. Med en

bakgrund inom informationssäkerhet är resultat i procent samt kronor troligtvis enklare att hantera än vad internränta är.

Även om en hel del negativt har tagits upp angående beräkningsmodellerna är det ändå nödvändigt att använda dem. En investering i IDS måste på något sätt vara lönsam om den skall genomföras, och det måste också gå att visa att den är lönsam, vilket beräkningsmodellerna kan användas till. Respondenten trycker i intervjun på att en viktig faktor är att cheferna måste ta ett beslut: ”Dom måste ta besluten om investeringarna. Köper du en IPS (Intrusion prevention system) idag är det en miljoninvestering. Framförallt om du har lite komplexare nätverk, så att det inte är ett enstaka företag i Sverige med bara en site.”. Beräkningsmodellerna blir nödvändiga verktyg att använda i en beslutsprocess. Modellerna kan användas för att visa dem som skall ta beslut om investeringar huruvida en investering i IDS är lönsam eller ej. På detta sätt är det möjligt att få t ex IT-chefens stöd i frågan kring en investering i IDS vara eller icke vara.

En annan intressant aspekt som bör tas upp är kompetensen hos företagen. Kompetensen är helt klart något som kan påverka resultatet från beräkningsmodellerna. T ex kanske ett företag vill investera i ett IDS som är open source. En sådan investering tar bort kostnaden för själva IDS:et (som även om det är en mindre kostnad absolut kan påverka resultatet). Å andra sidan ställer det krav på dem som skall ha hand om IDS:et. De måste besitta tillräcklig kompetens annars är risken att IDS:et kostar företaget mer än vad de tjänar på det. Respondenten berättar i intervjun gällande open source lösningar att: ”… du måste ha ganska hyfsad, eller ganska stor kunskap för att hålla igång grejerna… Du måste ha folk dygnet runt för att göra analyser om det verkligen är falskt, false positive, eller om det är ett riktigt larm.”. Kompetens är också något som kan påverka om ett företag skall köra IDS:et själva eller lägga ut driften. Ett företag som har kompetens att själva sköta driften för IDS tjänar troligen på att göra det jämfört med att lägga ut driften. Men vad händer om det visar sig att kompetensen inte är tillräcklig? Om ett företag har beräknat en vinst för investeringen kan denna vinst vändas till förlust. På frågan i intervjun om vad som är extra viktigt att tänka på vid investering i IDS svarar respondenten: ”Första frågan är ju egentligen, har du egen kompetens att ta hand om det?”. Frågan om kompetens skall alltså ses som viktig.

De interaktiva verktyg (se avsnitt 6.7) som tagits fram via arbetet med rapporten bör givetvis också diskuteras. Uppfattningen om verktygen är att de enkla att använda samt att de också är funktionsdugliga, det vill säga att de kan användas till att beräkna ROSI, NPV och IRR för en investering i IDS. Dock saknar verktygen viss automatik, de tar heller ingen hänsyn till beräkning samt uppskattning av indata, och dessutom är de relativt simpla i sin utformning. Ett alternativ till kalkylblad hade varit en webbapplikation. En webbapplikation hade troligtvis kunnat utformas till ett ganska avancerat verktyg, vilket hade kunnat erbjuda användaren mer valmöjligheter. T ex hade användaren kunnat ges möjligheten att på ett praktiskt sätt kunna utföra beräkningar på indata till beräkningsmodellerna. Indata hade kunnat lagras för att sedan vara möjlig att hämta när beräkningar med de olika modellerna skulle utföras. Ett webbaserat verktyg hade troligtvis också kunnat göras mer grafiskt och där med mer iögonfallande. De befintliga kalkylbladen duger dock väl för att kunna lönsamhetsbedöma investeringar i IDS. Dock hade fler funktioner, mer djup och ett mer grafiskt verktyg kunnat skapas via en webbapplikation.

Som avslutning i detta avsnitt görs en kortare reflektering över de relaterade arbeten som tas upp i avsnitt 2.3. I den mån det varit möjligt hade det varit intressant att

framförallt jämföra resultatet i denna rapport med den modell som Gordon & Loeb (2002) presenterar. I Gordon & Loebs modell skall det vara möjligt att avgöra den optimala summan att spendera för att skydda information. Det hade också varit intressant att utvärdera huruvida ”Cascading Threat Multiplier” hade påverkat resultaten från beräkningsmodellerna. ”Cascading Threat Multiplier” som introduceras av Iheagwara (2004) skall ge mer tyngd åt beräkningen av ALE.

8 Slutsats

Huvudfrågeställning som definierats i avsnitt 3 lyder: Hur kan ett mindre eller medelstort företag beräkna lönsamheten i att investera i IDS eller i att avstå, och när blir det lönsamt att införskaffa ett IDS? Utifrån huvudfrågeställningen kan ett antal slutsatser dras:

- Företag kan beräkna lönsamheten i att investera i IDS med hjälp av beräkningsmodellerna ROSI, NPV och/eller IRR, vilka bland annat beskrivs i avsnitten 6.1 – 6.3. Alla de tre modellerna har kriterier som gör att användaren av dem kan avgöra om en investering är lönsam. För ROSI handlar det om att få ett positivt procentvärde på investeringen. NPV ser något annorlunda ut, men även där handlar det om att få ut ett positivt värde, fast i kronor. För IRR gäller det att få ut ett värde som är lika med eller större än kalkylräntan. Företag som får ut positiva värden från beräkningsmodellerna för en viss investering i IDS kan alltså se investeringen som lönsam. I avsnitten 6.4 och 6.5 beskriver rapporten hur beräkningsmodellerna används.
- Precis som att företag kan beräkna om en investering i IDS är lönsam kan de också beräkna om det är lönsamt att avstå. Om värdena från ROSI, NPV samt IRR är negativa betyder det att investeringen ej är lönsam. Det vill säga att det kostar mer att investera i ett IDS än att inte göra det. Negativa värden från beräkningsmodellerna kan alltså tolkas som vad företag tjänar på att inte investera i IDS.
- Det blir (som punkterna ovan indikerar) lönsamt för företag att införskaffa IDS när beräkningsmodellerna resulterar i positiva värden, förutsatt att insamlad data till beräkningsmodellerna är korrekt och överensstämmer med verkligheten.

Med huvudfrågeställningen definierades också tre punkter som arbetet med rapporten skulle uppfylla:

1. Påvisa tillvägagångssätt som kan användas för att beräkna vad det kostar samt vad det inte kostar att införskaffa ett IDS, och hur tillvägagångssätten används.
2. Omständigheter kring beräkningen av lönsamheten skall tas i beaktning. T ex om det finns några svårigheter runt beräkningarna, eller andra faktorer som påverkar dem.
3. Ett interaktivt verktyg skall implementeras. Med det interaktiva verktyget är det meningen att en användare skall kunna göra ekonomisk bedömning för införskaffande av IDS

Den första punkten uppfylls i avsnitten 6.1 – 6.5. Där beskrivs beräkningsmodellerna ROSI, NPV samt IRR, och det skildras också hur de används. Kostnaden av att inte införskaffa ett IDS gestaltas i rapporten av ALEuSi. ALEuSi beskrivs närmare ibland annat avsnitten 6.1, 6.4 samt 6.5 och diskuteras också i avsnitt 7.2.

Punkt två uppfylls bland annat genom att datainsamlingsfasen tas upp i avsnitt 6.4. Där beskrivs hur indata till beräkningsmodellerna kan samlas in. I diskussionen av resultatet (se avsnitt 7.2) tas också datainsamlingen upp, där bland annat svårigheterna och vikten av datainsamlingen diskuteras. Med den här punkten kan också slutsatsen dras att även om beräkningsmodellerna i sig är relativt enkla i sin utformning är användandet av dem inte helt okomplicerat. Det vill säga att bedöma investeringar i

IDS kräver mer än att bara förstå hur beräkningsmodellerna används. Det gäller också att förstå vikten av arbetet kring beräkningsmodellerna för att de skall gå att utnyttja på ett bra sätt.

Tredje punkten uppfylls via de kalkylblad som skapats i Microsoft Excel. Med kalkylbladen är det möjligt för en användare att göra ekonomiska bedömningar med ROSI, NPV samt IRR vid en investering i IDS, vilket beskrivs närmare i avsnitt 6.7.

Utöver den definierade frågeställningen och de efterföljande punkterna går det att dra ytterligare slutsatser:

- ROSI, NPV samt IRR är beroende av insamlandet av data. Det är nödvändigt för företag som vill beräkna lönsamhet vid investering i IDS att de vet hur de ska göra. Det vill säga att de vet vilka kostnader som skall tas med samt hur de skall få fram kostnaderna.
- Kostnaderna som tas fram under datainsamlingen till beräkningsmodellerna påverkar resultatet. En beräkning för en investering i IDS som precis ger ett positivt värde kan påverkas åt båda hållen. Låt säga att IDS:et antas upptäcka 85 % av alla intrång. När IDS:et tas i drift visar sig den siffran vara 70 %. En positiv beräkning kan då svänga till en negativ.
- Företag som skall investera i IDS kan få mycket att fundera över. Vad kostar ett intrång? Vad kostar det att agera när IDS:et larmar? Vad kostar ett falskt alarm? Vilka hot kan IDS:et skydda mot? Skall företaget i fråga själva ha hand om IDS:et eller skall den tjänsten läggas ut? Med mera. Det finns alltså en mängd frågor som behöver redas ut. Frågor som alla påverkar kostnaderna.
- Den största delen (eller hela om IDS:et är open source) av investeringskostnaden står handhavandekostnaden för. Det är också något som Ulf Mäkitalo nämner i intervjun: ”…minsta kostnaden är ju egentligen inköpet, som jag ser på det. Den stora är ju att ta hand om systemet, förvaltning av systemen.”.

Sammanfattande slutsats baserat på resonemanget i diskussionen (se avsnitt 7.2) och slutsatserna i detta avsnitt: Beräkningsmodellerna är relativt enkla i sin utformning, men indata till dem kan vara komplicerad att få fram. Många uppskattningar behöver göras för indata, och alla värden påverkar mer eller mindre resultaten. Det finns också många frågor att ta ställning till. Min uppfattning är dock att beräkningsmodellerna är nödvändiga vid investeringar i IDS, dels för att kunna ta fram ett resultat för en viss investering, och dels för att kunna visa resultatet för dem som skall ta beslut om investeringen är lönsam eller ej.

9 Förslag till fortsatt arbete

När denna rapport påbörjades fanns det en förväntan på att tillvägagångssätten som söktes för att lönsamhetsbedöma investeringar i IDS skulle vara ganska komplexa. Resultatet blev de tre beräkningsmodellerna ROSI, NPV samt IRR, vilka i sig inte är särskilt komplexa. Däremot har det under arbetet med rapporten kommit fram att datainsamlingsfasen för beräkningsmodellerna är desto mer komplex. Därför hade ett eventuellt fortsatt arbete inom detta område kunnat vara att undersöka datainsamlingsfasen mer noggrant. Ett sådant arbete hade varit intressant dels då det är värdena från datainsamlingen som påverkar beräkningarna med modellerna, och dels för att datainsamlingsfasen också är väldigt viktig när det gäller att lönsamhetsbedöma investeringar i IDS.

Ytterligare fortsatt arbete hade kunnat vara att vidareutveckla det interaktiva verktyget genom att t ex göra det mer avancerat.

Referenser

Andersen, V. & Gamdrup, P. (1994) Forskningsmetoder. I: H. Andersen (red), *Vetenskapsteori och metodlära – En introduktion*. (s. 68-94). Fredriksberg: Samfundslitteratur.

Axelsson, S. (2000a) *Intrusion Detection Systems: A Survey and Taxonomy*. Department of Computer Engineering, Chalmers University of Technology, Göteborg.

Axelsson, S. (2000b (22)) The Base-Rate Fallacy and the Difficulty of Intrusion Detection. *ACM Transactions on Information and System Security, 3*, 186-205.

Bankovic´, Z., Stepanovic´, D., Bojanic´ , S. & Nieto-Taladriz, O. (2007) Improving network security using genetic algorithm approach. *Computers and Electrical Engineering, 33*, 438-451.

Bell, J. (2000) *Introduktion till forskningsmetodik*. (3:e upplagan) Buckingham: Open University Press.

Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B. (2008) *Thesis Projects – A Guide for Students in Computer Science and Information Systems*. (2:a upplagan) London: Springer-Verlag London Limited.

Bojanc, R. & Jerman-Blažič, B. (2008) Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces, 30*, 216-222.

David, J.S., Schuff, D. & St. Louis, R. (2002) Managing your IT total cost of ownership. *Communications of the ACM, 45*, 101-106.

Davis, A. (2005) Return on security investment – proving it's worth it. *Network Security, November*, 8-10.

Depren, O., Topallar, M., Anarim, E. & M. Ciliz, M. (2005) An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. *Expert Systems with Applications*, *29*, 713-722.

Fumey-Nassah, G. (2007) The Management of Economic Ramification of Information and Network Security on an Organization. Presenterat vid: *Information Security Curriculum Development Conference'07*, Kennesaw 28-29 September, 2007.

Gordon, L. & Loeb, M. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security, 5*, 438-457.

Gordon, L. & Loeb, M. (2006) Budgeting Process for Information Security Expenditures. *Communications of the ACM, 49*, 121-125.

Iheagwara, C. (2004) The effect of intrusion detection management methods on the return on investment. *Computers & Security, 23*, 213-228.

Iheagwara, C., Blyth, A. & Singhal, M. (2004) Cost effective management frameworks for intrusion detection systems. *Journal of Computer Security, 12*, 777-798.

Kanlayasiri, U. & Sanguanpong, S. (2002) *Network-based Intrusion Detection Model for Detecting TCP SYN flooding*. Department of Computer Engineering, Kasetsart University, Bangkok, Thailand.

Labib, K. (2004) Computer Security and Intrusion Detection. *The ACM Student Magazine*.

Lee, W., Fan, W., Miller, M., Stolfo, S. J. & Zadok, E. (2002) Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security, 10*, 5-22.

Lei, K. & Rawles, P. (2003) Strategic Decisions On Technology Selections for Facilitating A Network/Systems Laboratory Using Real Options & Total Cost of Ownership Theories. Presenterat vid: *CITC4'03*, Lafayette 16-18 Oktober, 2003.

Loeb, M. (2002) *Return on information security investments: Myths vs. Realities*. Strategic Finance. Tillgänglig på Internet: http://www.allbusiness.com/technology/services-systems-analysis-services/323886-1.html [Hämtad: 09.02.20].

Lönnqvist, R. (2005) Investeringskalkyler. I: U. E. Olsson (red.), *Kalkylering för produkter och investeringar* (3:e upplagan) (s. 209-254). Lund: Studentlitteratur.

Newman, D., Snyder, J. & Thayer, R. (2002) *Crying wolf: False alarms hide attacks*. Network World. Tillgänglig på Internet: http://www.networkworld.com/techinsider/2002/0624security1.html [Hämtad: 09.02.22].

Patcha, A. & Park, J. (2007) An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, *51*, 3448-3470.

Richardson, R. (2008) (2008) *CSI Computer Crime & Security Survey - The latest results from the longest-running project of its kind*. CSI Computer Crime and Security Survey. Tillgänglig på Internet: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf [Hämtad: 09.01.22]

Sobh, T. (2006) Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. *Computer Standards & Interfaces, 28*, 670-694.

UcedaVelez, T. (2008) What's the Return on Your Security Investment? *The Journal of Corporate Accounting & Finance*, *July/August*, 61-67.

Wei, H., Frinke, D., Carter, O. & Ritter, C. (2001) Cost-Benefit Analysis for Network Intrusion Detection Systems. Presenterat vid: *CSI 28th Annual Computer Security Conference 2001*, Washington, D.C. October 29-31, 2001

Werlinger, R., Hawkey, K., Muldner, K., Jaferian, P. & Beznosov, K. (2008) The Challenges of Using an Intrusion Detection System: Is It Worth the Effort? Presenterat vid: *Symposium On Usable Privacy and Security (SOUPS) 2008*, Pittsburgh 23-25 Juli, 2008.

Ye, N., Farley, T. & Lakshminarasimhan, D. (2006) An attack-norm separation approach for detecting cyber attacks. *Information Systems Frontiers*, *8*, 163-177.

Zhang, Y., Lee, W. & Huang, Y. (2003) Intrusion Detection Techniques for MobileWireless Networks. *Wireless Networks*, *9*, 545-556.

Zhengbing, H., Zhitang, L. & Junqi, W. (2008) A Novel Network Intrusion Detection System(NIDS) Based on. Presenterat vid: *e-Forensics 2008*, Adelaide 21-23 Januari, 2008.

Bilaga A – Förkortningar

ALE – ”Annual loss expectancy”. Den årliga förväntade förlusten.

ALEmSi – ALE med säkerhetsinvestering.

ALEuSi – ALE utan säkerhetsinvestering.

ARO – ”Annual rate of occurrence”. Det antal gånger en viss risk förväntas ske per år.

AV – ”Asset value”. Värdet på en tillgång.

EF – ”Exposure factor”. Hur mycket ett realiserat hot kan orsaka i förlust för en viss tillgång.

HIDS – ”Host-based” intrångsdetekteringssystem.

IDS – Intrångsdetekteringssystem.

IRR – ”Internal rate of return”. Beräkningsmodell för internräntan på en investering.

NIDS – ”Network-based” intrångsdetekteringssystem.

NPV – ”Net present value”. Beräkningsmodell för nuvärdet på en investering.

ROI – ”Return on investment”. Beräkningsmodell för avkastningen på en investering.

ROSI – ”Return on security investment”. Se ROI.

SLE – “Single loss expectancy”. Den totala summan av intäkten som förloras vid en enskild förekomst av en viss risk

TCO – ”Total cost of ownership”. Modell för att beräkna den totala ägandekostnaden.