2005:229 SHU

EXAMENSARBETE

Varför används inte en nationell IT-incidenthanteringsorganisation?

En studie av rutiner vid incidentrapportering

Andreas Palo

Luleå tekniska universitet

Systemvetenskap
D-nivå
Institutionen för Industriell ekonomi och samhällsvetenskap
Avdelningen för Systemvetenskap

2005:229 SHU - ISSN: 1404-5508 - ISRN: LTU-SHU-EX--05/229--SE

Abstract

This thesis discusses reporting of IT incidents. I have investigated routines that are necessary for reporting IT incidents from different organisations to Sitic, the IT incident centre in Sweden. The background for this thesis is that the reporting to Sitic has been slow started. I have investigated which routines that could make the cooperation better. The result has shown that there is lack of some routines on both sides. The organisations wish that the reporting could be more automatic and that the advices and warnings they get from Sitic should be more specific for their needs. Another result that have been known is that organisations already cooperate with other security companies and therefore they do not see any need to also cooperate with Sitic. Nevertheless, the organisations are positive of Sitic as a coordinating organisation.

Sammanfattning

Denna uppsats behandlar rapportering av IT-incidenter. Mer specifikt har jag undersökt vilka rutiner som behövs för att organisationer på ett bra sätt ska kunna rapportera incidenter till Sitic, Sveriges IT-incidentcentrum. Bakgrunden till uppsatsen är att rapporteringen till det relativt nya Sitic har varit trögstartad. Jag har undersökt vilka rutiner som bör finnas hos de rapporterande organisationerna och hos Sitic för att få till stånd ett effektivare samarbete. Resultatet har visat på att det finns brister i en del rutiner på båda sidor av förhållandet. Respondenterna önskade en enklare automatiserad rapportering och mer riktade råd och varningar från Sitic som bättre uppfyllde deras behov. Ett annat resultat av undersökningen är att många företag redan idag har ett fungerande utbyte av incidentinformation med andra organisationer och ser därför inte något akut behov av att rapportera till ett nationellt centrum. Företag ser dock i stort sett positivt på Sitic i samordningssyfte.

Förord

Denna uppsats är ett resultat av ett examensarbete på D-nivå på 10 poäng i systemvetenskap vid institutionen IES, vid Luleå tekniska universitet.

Uppsatsen behandlar förutsättningarna för ett fungerande samarbete mellan Sitic och andra organisationer för incidenthantering.

Jag vill passa på att tacka de företag och organisationer som har medverkat vid mina intervjuer. Jag vill även tacka min handledare Jörgen Nilsson för värdefulla diskussioner.

Luleå i oktober 2005

Andreas Palo

Innehållsförteckning

1 Inledning

I detta första kapitel kommer jag inledningsvis att presentera bakgrunden till uppsatsämnet. Sedan kommer en problemdiskussion som leder till forskningsfrågan och syftet med uppsatsen. Slutligen beskriver jag vilken teori som jag tänker ta upp och förklarar begrepp som används i uppsatsen.

1.1 Bakgrund

Människan har alltid strävat efter att kunna kommunicera på ett snabbt sätt oavsett avstånd. Detta har möjliggjorts på ett kraftfullt sätt med dagens teknik, i synnerhet tack vare Internet. Informationsteknikens utveckling har emellertid också medfört ökade säkerhetsproblem.

IT-incidenter leder till problem för många företag idag. Eftersom informationen är många företags viktigaste tillgång krävs det att informationen är säkrad på olika sätt. För att informationen skall anses säker skall den uppfylla följande krav som Statsverket med flera nämner: tillgänglighet, sekretess och riktighet. Dessa aspekter försöker olika verksamheter uppnå med ett antal tekniska och administrativa skyddsåtgärder.

Trots att verksamheterna har vidtagit olika åtgärder, utsätts de för olika hot i form av attacker, virus, misstag mm, som leder till att arbetet försämras och ineffektiviseras. För att dessa problem skall kunna åtgärdas och förebyggas, måste incidenterna hanteras på ett sådant sätt att de kan åtgärdas och förebyggas. I detta ingår att rapportera incidenterna till personer och organisationer som har möjlighet att åtgärda problemen.

Incidentapportering sker till största del inom organisationerna. I många industriländer har det dock sedan 1990-talet även funnits nationella oberoende incidenthanteringsorganisationer, vanligtvis benämnda CERT. Dessa har till uppgift att ta emot incidentrapporter från alla samhällets delar och med hjälp av dessa ge ut statistik, varningar och råd om vilka åtgärder som organisationer behöver vidta för att säkra sin information.

Under år 1998 började frågan om en svensk nationell IT-incidenthanterings-organisation att utredas. Det fanns då en oklarhet om hotbilden för informationsoperationer och IT-incidenter. Det saknades även svensk statistik på IT-incidenter. Det var därför angeläget att en systematisk IT-incidentrapportering och hotbildsanalys kom igång. [CHR02]

Telia och SUNET har redan sedan några år tillbaka bedrivit CERT-verksamheter. Däremot har det inte funnits någon central IT-säkerhetsorganisation i Sverige som sammanställt inträffade incidenter och analyserat hot och risker. Svenska myndigheter och företag har därför fram till årsskiftet 2002/2003 varit hänvisade till att erhålla varningar och att hämta information om sårbarheter från utländska organisationer. [CHR02]

Under åren 1998-2002 gjordes ett antal utredningar om hur en sådan organisation skulle se ut. Post- och telestyrelsen (PTS) är de som på uppdrag av regeringen utrett förutsättningarna för en sådan funktion för IT-incidentrapportering i Sverige. Denna funktion skulle syfta till att motverka angrepp på IT-system och datanät. Tänkbara angripare skulle kunna vara såväl stater som företag, kriminella organisationer, terrorister och enskilda individer. Mot bakgrund av denna undersökning fick PTS den 30 maj 2002 i uppdrag av regeringen att inrätta en nationell funktion för IT-incidentrapportering. [CHR02]

Utredningarna resulterade i ett inrättande av Sitic, Sveriges IT-incidentcentrum. Sitic är relativt nytt (start januari 2003) och har uppgiften att hjälpa i huvudsak statliga myndigheter, kommuner, landsting, men också privata företag i deras IT-säkerhetsarbete [PTS05].

Sitics arbete bygger delvis på att olika verksamheter frivilligt rapporterar om IT-incidenter som de drabbas av. Sitics uppgifter är därefter att stödja samhället i arbetet med skydd mot IT-incidenter. De skall också främja informationsutbytet om IT-incidenter mellan samhällets organisationer och sprida information om nya problem som kan störa IT-system. De lämnar också ut information och råd om förebyggande åtgärder samt sammanställer och ger ut statistik. [SIT05]

Syftet med ett centralt stöd för IT-incidenthantering är, enligt utredningen, att i realtid eller nära realtid se till att attacker mot datasystem avstyrs och upphör, samt stödja återställande av systemen vid större attacker hos företag. Incidentstödet skall ha översikt och kunskap om IT-hot och IT-säkerhet utifrån ett helhetsperspektiv. En central IT-incidenthanteringsfunktion ska ha den förmåga som krävs för att skilja okvalificerade och osystematiska intrångsförsök från kvalificerade och systematiska angrepp. Säkerhetsproblem som oklara fel, större avvikelser, incidenter och återstart av system som inte klaras ut av enskilda systemägare skall kunna hanteras. Kvalificerad rådgivning från en hjälpcentral skall kunna lämnas. Det yttersta ansvaret skall dock ytterst kvarstå hos systemägaren. [CHR03]

För att organisationer skall kunna skydda sin verksamhet måste kunskap om hot, sårbarheter och råd om åtgärder komma in i organisationen på något sätt. Den informationskällan skulle kunna vara och är också i många fall olika IT-incidenthanteringsorganisationer.

För att säkerställa den nationella säkerheten finns det som tidigare nämnt nationella IT-incidentorganisationer i många länder. Syftet med dessa organisationer är att skapa ett öppet forum för IT-incidenter som alla samhällets delar kan ha nytta av genom att rapportera till och ta del av.

1.2 Problemdiskussion

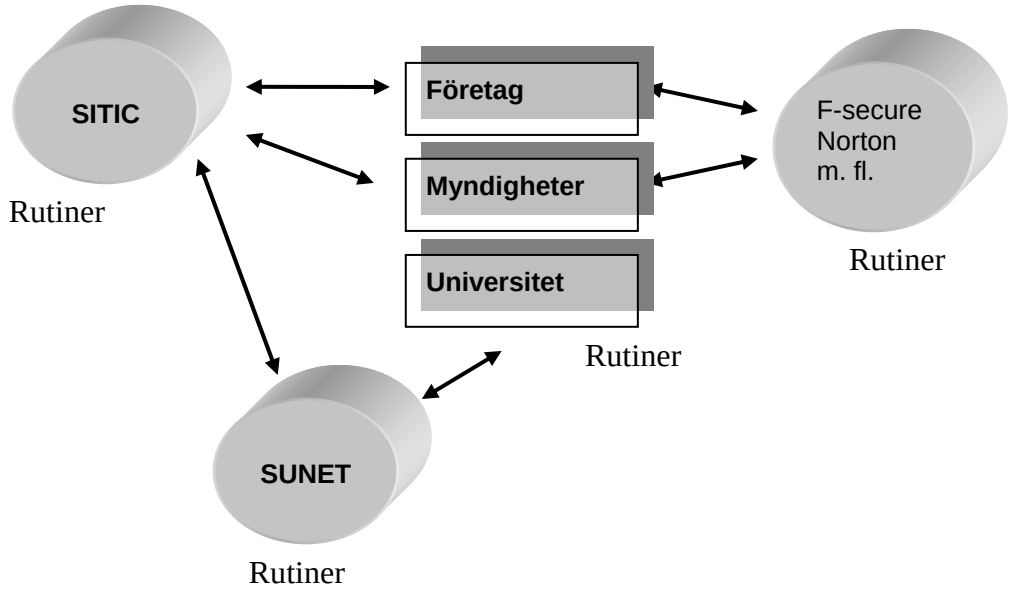
Den första tiden efter att Sitic startats har inte fortlöpt som önskat enligt kritiker utanförför Sitic. En artikel i tidningen Ny Teknik nämner att inrapporteringen till Sitic har varit trögstartad. Efter de tre första månaderna hade bara en rapport kommit in. Eftersom Sitic bygger en stor del av arbetet på organisationers

inrapportering tycker Staffan Karlsson, chef för samordningen av Sveriges IT-säkerhetsarbete på myndighetsområdet, att det är ett problem. Han tror dock att detta beror på att det inte funnits något skydd i sekretesslagen som täcker in den här typen av information. Någon annan nämner i en artikel att Sitic varit sena med att varna för nya hot som har uppkommit. [NYT05]

Den första juli 2004 trädde en ändring i sekretesslagen i kraft. Ändringen väntades öka möjligheterna för Sitic, att få in rapporter om IT-incidenter eftersom Sitic då kunde börja sekretessbelägga rapporter som bedöms känsliga ur sekretessynpunkt, vilket inte gick att göra tidigare beroende på offentlighetsprincipen. Att flera organisationer vågar lämna rapporter ger Sitic ett bättre beslutsunderlag för de varningar de skickar ut till organisationer och företag. Dessutom kan en ökad rapportering bidra till snabbare varningar.

Av någon anledning väljer företag och myndigheter att inte rapportera incidenter i den utsträckning som Sitic hade väntat sig. Jag frågar mig därför varför inte organisationer rapporterar till och använder sig av Sitic. Denna avsaknad av rapportering kan bero på en rad olika saker. Jag kommer att rikta in mig på de rutiner och rapporteringsstöd som organisationerna i detta förhållande använder sig av.

Av ovanstående problemdiskussion har jag gjort en illustration över hur incidentrapporteringen ser ut i Sverige idag. Alla organisationer har något slags samarbete med någon incidenthanteringsorganisation. Samtliga organisationer har därför också rutiner för dessa samarbeten.



Figur 1. Relationer inom incidenthantering

1.3 Forskningsfråga

Vilka rutiner bör finnas hos organisationer och incidenthanteringsorganisationer för att främja incidentrapportering?

1.4 Syfte

Jag vill, med tanke på låga rapporteringssiffrorna, undersöka vilka rutiner Sitic och inrapporterande organisationer bör ha för att få till ett fungerande utbyte av incidentinformation. Jag kommer också att undersöka hur väl företagen känner till Sitic, om organisationerna använder sig av andra kanaler, vilka eventuella hinder som finns och om företag överhuvudtaget ser fördelar med att rapportera och ta emot incidentinformation från en organisation av Sitics karaktär. Jag kommer att titta på vilka rutiner Sitic har för att hantera insamlad incidentinformation samt rutiner för kommunikation med eventuella inrapportörer.

Jag ska undersöka dels hur rutinerna kan åtgärdas och hur ett rapporteringssystem bör se ut enligt litteratur och respondenter. Jag vill också undersöka relevansen med en nationell incidenthanteringsorganisation.

Resultatet av rapporten kommer att visas i form av en teoripresentation och i form av en analys av en empirisk undersökning.

1.5 Rapportens innehåll

Uppsatsen innehåller avsnitten inledning, teori, metod, empiri, analys, resultat, metoddiskussion och diskussion.

I teoridelen kommer följande områden att presenteras:

- Incidentbegreppet
- Teori om rapportering (syfte, krav, rutiner)
- Teori om kunskapshantering (i synnerhet kunskapsdelning)
- Rutiner för incidenthantering

Jag kommer i kapitel tre att presentera den metod jag använder mig av för att producera uppsatsen. I kapitel fyra återfinns den empiriska undersökning, som jag i kapitel fem analyserar och jämför mot teorin. Resultatet av uppsatsen presenteras i kapitel sex. En metoddiskussion finns i kapitel sju. Slutligen består kapitel åtta av en allmän diskussion över hela rapportens innehåll.

1.6 Avgränsningar

Denna rapport behandlar området rapportering av IT-incidenter. Området kunskapsdelning kommer också att behandlas, då rapportering av IT-incidenter handlar om att sprida incidentinformation till olika intressenter. Rapporten

förklarar dels vad rapportering innebär och om olika verksamheters syn på och erfarenheter av rapportering till ett centralt IT-incidentcentrum.

Jag kommer i huvudsak undersöka hur organisationers rutiner ser ut vad gäller rapportering till en central myndighet, det vill säga extern rapportering. Jag kommer även till en viss del gå in på rapporternas innehåll och utformning.

De incidenter som incidentrapportering i den här uppsatsen syftar på, är av sorten avsiktliga attacker via Internet. Jag kommer med andra ord inte att behandla incidenter av typen misstag, komponentfel och vanliga driftstörningar.

De verksamheter jag tänker ta med i den empiriska undersökningen skall vara beroende av informationsteknologi till den grad att problem som uppstår i datorsystem kan vara av verksamhetskritisk karaktär.

1.7 Förklaring av begrepp

CERT *Computer Emergency Response Team*
CERT är en global organisation för att hantera allvarligare IT-säkerhetsincidenter och har sitt ursprung i USA. CERT arbetar på nationell nivå.

CERT har som mål att stärka säkerheten på sidor på Internet. Detta sker genom att de larmar för säkerhetsbrister, undersöker förändringar i nätverkssystem på lång sikt, mm. De har även intresse för att incidenter rapporteras in till dem, så att de kan sammanställa denna information för att kunna utbilda och varna organisationer och stärka deras säkerhet. [CER05]

Begreppet CERT används numera som en allmän beteckning på alla sorters incidenthanteringsorganisationer.

IT-incident
Med IT-incident menas i denna rapport en incident som drabbar ett datorsystem så att brister som påverkar ett eller flera av de nämnda säkerhetskraven uppstår. De incidenter som åsyftas i denna uppsats är av typen avsiktliga attacker, incidenterna är exempelvis inte orsakade av misstag eller fel i komponenter.

Portscanning
Detta begrepp innebär att någon letar efter öppna portar på datorer som ligger uppkopplade på nätet, för att om möjligt försöka göra ett intrång i datorn eller nätverket.

SANS (SysAdmin, Audit, Network, Security)
Sans är ett amerikanskt institut som tillhandahåller utbildning och utveckling inom IT-säkerhetsområdet.

SUNET
SUNET är en samverkan mellan högskolorna i Sverige och finns till för att främja datakommunikation som är till för högskolorna, i första hand genom att tillhandahålla möjligheter till datakommunikation till/från/mellan universitet och högskolor. Bedriver även en egen CERT dit aktörerna på Sunets nät rapporterar incidenter.

Abuse-anmälan
En abuse-anmälan skriver man i syfte att rapportera missbruk av nättjänster av något slag. Anmälan skickas till nätägaren och innehåller typ av incident, IP-nummer samt tidpunkt då händelsen inträffat.

2 Teori

Den inledande delen av teorin kommer att behandla incidenter samt rapportering av incidenter. Där kommer krav på rapportering, rutiner och syftet med rapportering att presenteras. Jag kommer sedan att ta upp teori om kunskapshantering och informationsdelning organisationer emellan.

2.1 Vad är en incident?

Incidenter är grunden till incidentrapportering, eller med andra ord orsaken till den. Därför är det av intresse att utreda vad olika forskare och författare lägger för innebörd i ordet incident.

Oscarson [OSC01] menar att en IT-incident är en händelse som påverkar en verksamhets informationstillgångar på ett negativt sätt. Oscarson säger också att det ofta är svårt att skilja på ett hot och en incident, han menar att skillnaden ligger i tidsperspektivet. Ett hot är något som kan komma att inträffa i framtiden, medan en incident är något som händer nu eller som har inträffat tidigare. Ett hot som realiseras blir därför en incident.

Om incidenten får negativa konsekvenser på informationstillgångarna räknas den som en skada.

En incident kan vara av skiftande slag. Information kan förändras på ett okontrollerat sätt, någon obehörig försöker komma åt information eller informationen kan bli oåtkomlig för behöriga. Dessa skador kan kopplas till de tidigare nämnda kraven på information; sekretess, riktighet och tillgänglighet.

IT-incidenter betecknas i Post och telestyrelsens rapport om IT-incidenthantering som en eller flera händelser som:

- drabbar eller påverkar IT-system, inklusive system för datakommunikation, eller där IT-system utnyttjas i annan oönskad verksamhet
- är oönskade och oplanerade ur ägarens eller förvaltarens perspektiv
- direkt eller indirekt medför eller kan medföra allvarliga konsekvenser för ägare, användare eller andra

På Sitics hemsida står det att en incident är ”en verklig eller uppfattad händelse av säkerhetskritisk karaktär i en dator eller ett nätverk”. De nämner också mer specifikt att de med incidenter avser avsökningar, intrång och tillgänglighetsattacker. Interna handhavandefel och fysiska hot som brand och stöld är inte exempel på incidenter enligt denna definition. [SIT05]

CERT benämner en incident som en händelse som motverkar en säkerhetspolicy. Följande händelser är exempel på sådana.

- Försök att erhålla obehörig access till system eller dess information
- Avbrott eller blockering av tjänster
- Obehörig användning för körning och lagring av data
- Förändring av hård- och mjukvara utan ägarens kännedom eller tillåtelse. [CER05]

2.2 Incidentrapportering

I alla organisationer och företag är information värdefull. För att den ska komma till nytta måste den dock finnas på rätt ställe vid rätt tidpunkt. Att en säkerhetsincident inträffat måste rapporteras till berörda, helst så fort incidenten upptäckts. Berörda kan vara driftansvariga för det attackerade systemet, men även kunder till företaget. Ett datoriserat system är idealiskt för att göra denna rapportering effektiv. [MAN01]

Incidentrapportering är ett strategiskt verktyg för informationssäkerhet. Genom att ta reda på vilka aktuella hot och risker som finns kan företaget få underlag för informationssäkerhetsstrategin. Hot är ju en av de mest centrala delarna i all sorts säkerhetsarbete. Vilka hot som finns är därför avgörande för vilken strategi organisationer har och vilka åtgärder som vidtas för att säkerställa verksamheten. [MIT03]

Med hjälp av information från inrapporterade misstänkta beteenden i IT-miljön kan nätverksadministratören identifiera möjliga intrång eller intrångsförsök. Information från incidentrapporteringen kan även användas för att besluta om övervakningen av det interna nätverket bör höjas och om man ska lägga ner mer jobb på att analysera säkerheten i nätverket [ALL01].

2.2.1 Intern rapportering

Detaljerad rapportering ger ett mycket viktigt underlag för att avgöra vad som skett vid misstanke om säkerhetsrelaterade incidenter. Desto fler detaljer som rapporteras desto större är sannolikheten att den önskade informationen går att återfinna. Dock finns det praktiska problem i samband med incidentrapportering. Först och främst måste man vara på det klara med vad som skall rapporteras. Rapporteras för mycket riskerar man att överhopas av data och få hanteringsproblem vid analys och uppföljning av inträffade incidenter. Det är därför av stor vikt att noggrant definiera vilka händelser som skall rapporteras och detaljeringsgraden på rapporterna.

Utöver detta måste olika rutiner etableras inom organisationen. En användare kan inte åläggas att i detalj redovisa orsakerna bakom en händelse. Lika naturligt är det att ansvarig inom driften skall kunna redovisa vilka skyddsåtgärder som finns

och hur dessa fungerat i samband med en inträffad händelse. Det måste alltså finnas en ansvarig grupp/person utsedd för att samordna incidenthanteringen.

Den tredje viktiga delen för att etablera en bra incidenthantering inom en organisation är att all personal vet hur man skall agera vid misstanke om en incident. Det kan handla om alltifrån att säkerhetskopiera till att kontakta rätt person.

Det finns i stora drag en naturlig rapporteringskedja som dessutom belyser olika detaljeringsnivåer och informationsinnehåll i rapporterna. [ÖCB05]

- Användare till driften
- Driften till ansvarig för incidenthantering
- Ansvarig för incidenthantering till ledningen

Genom att utföra rapportering får den rapporterande kunskap om hur olyckor uppstår och i en förlängning också om hur man kan undvika dessa. [ALL01]

När en säkerhetsincident har inträffat måste den rapporteras till berörda, helst så fort incidenten upptäckts. Berörda kan vara driftansvariga för det attackerade systemet, men även kunder till företaget. Ett datoriserat system är idealiskt för att göra denna rapportering effektiv. [MAN01]

2.2.2 Extern rapportering

Incidentrapportering kan ske både internt och externt, exempelvis till CERT-organisationer. Det är viktigt att informera andra organisationer om incidenter. Säkerhetsorganisationer i olika företag kan då arbeta förebyggande genom att ta del av andras incidenter. Allen föreslår därför att incidenter även skall rapporteras till någon organisation som arbetar med att förmedla denna information, se CERT-definitionen. [ALL01]

Det finns dock svårigheter med att få företag och myndigheter att rapportera incidenter i verksamheten till externa aktörer. Det beror dels på att företag (särskilt inom näringslivet) vill skydda sitt goda namn dels att det tar mycket tid och resurser i anspråk. Detta medför ett stort mörkertal av inträffade incidenter. [CHR03]

Det finns åtminstone tre syften med rapportering av IT-säkerhetsincidenter till externa incidentorganisationer, följande syften nämns i en statlig utredning angående inrättandet av en nationell IT-hanteringsorganisation i Sverige. Proposition 2001/02:158 *”Samhällets säkerhet och beredskap”*.

1. Den som rapporterar incidenterna kan erhålla hjälp med att bemöta dem.

2. Rapportering sker för att kunna varna andra för exempelvis hot som finns för tillfället.

3. Rapportering för statistik, som utgör ett väsentligt underlag till exempel för att identifiera och urskilja samordnade attacker på bred front mot Sverige och mot nationella säkerhetsintressen. [CHR03]

2.2.3 Rapporteringsplikt

För att upptäcka en avancerad samlad informationsattack mot Sverige behövs det enligt en utredning en stor volym rapporterade. Därför anser en utredning, SOU 2001: 41 *”Säkerhet i en ny tid”*, att statliga myndigheter bör åläggas en skyldighet att rapportera samtliga inträffade IT-säkerhetsincidenter till IT-incidenthanteringsfunktionen. Sådana skyldigheter finns både i USA och i Storbritannien.

2.2.4 Rutiner vid rapportering

IT-kommissionen [ITK05] har tagit fram en åtgärdslista som myndigheter bör använda sig av när de drabbas av incidenter.

En fiktiv händelse kan ha följande förlopp:

1. En incident inträffar vid en myndighet
2. Incidenten rapporteras enligt interna rutiner
3. Incidenten hanteras och utreds
4. Beslut fattas lokalt om incidenten är av sådan art att den ska rapporteras till polisen, med påföljande brottsanmälan
5. I de fall incidenten är av sådan art att inrapportering bör ske upprättas en incidentrapport enligt mall
6. Rapport översänds skyddad till funktionen för incidenthantering
7. Rapporten kategoriseras och införs i register hos funktionen
8. Incidenten redovisas i statistikrapporter.

IT-kommissionen är medveten om att många myndigheter saknar rapporteringsrutiner för interna incidenter och påpekar att det är något som varje organisation måste skapa rutiner för.

En snabb inrapporteringsrutin är viktig. Det behövs för att kunna spåra intrång. Loggar sparas endast under en viss tid. För att få de anställda att rapportera incidenter krävs det att rapporteringen är enkel och snabb att utföra. [JOH02] I organisationens IT-säkerhetspolicy ska det stå vart och var de anställda ska rapportera incidenter. [ALL01]

Kommunikation och kontakter

Det finns många fördelar med att peka ut enstaka kontaktpersoner inom ett incidentteam i en organisation och låta dessa sköta alla kontakter med omgivningen. Det man vinner är bland annat kontroll över vilken information som lämnas ut och till vilka. Innan kontakter med rättsväsendet eller andra externa

parter sker bör man vara säker på att berörda verksamhetsansvariga är informerade och har gett klartecken.

Tänkbara externa kontakter är bland annat:

- incidenthanteringsorganisationer, t.ex. CERT/CC och dess svenska motsvarighet, Sitic
- organisationer varifrån attackerna kommer,
- organisationer dit spåren leder (t.ex. om man hittar adresser eller domännamn i loggfiler och programkod),
- andra som blivit drabbade,
- tele- och nätverksleverantörer.

Vid dessa kontakter måste det vara klart vilken information som kan lämnas ut. Det kan t.ex. vara känsligt att berätta om vilka andra som blivit drabbade eller beskriva i detalj hur den egna organisationen blivit angripen.

Om andra har blivit drabbade anses det som god sed i Internetvärlden att kontakta dem direkt. Inom vissa organisationer eller i samband med vissa typer av incidenter kan detta dock vara svårt eller till och med strida mot gällande regler. Någon gång under det inträffade kan det bli nödvändigt att gå ut med information till en större krets, till exempel de datoransvariga inom företaget eller alla anställda. [STA05]

Dokumentera

Att dokumentera incidenter är av stor vikt för att kunna förbättra säkerheten i en organisation. För att göra sådana dokument krävs det rutiner, dessa rutiner underlättas med ett incidentrapporteringssystem. Enligt Statskontoret kan incidentrapporteringen även göra att mytspridning och ryktesspridning undviks. [ALL01]

Om det inte finns dokumenterat har det aldrig hänt sägs det. För att undvika missar i kommunikationen och för att få underlag i det akuta, men även framtida, arbetet bör man dokumentera alla händelser och allt runtomkring.[STA05]

2.2.5 Rapporteringssystem

Rapporter kan vara olika detaljerade beroende på den rapporterandes kunskaper och erfarenheter. Enligt SANS (se begreppsförklaring) måste åtminstone följande uppgifter rapporteras in för att man ska kunna arbeta med en incident:

- Datum
- Tidpunkt
- Rapportör
- Beskrivning av den eventuella incidenten.

Hur det rapportsystem ser ut, i vilket man ska lämna ovanstående uppgifter, kan vara olika på olika ställen och beroende på vilken sorts incidenter det handlar om. Författare diskuterar dels hur formulär ska vara utformat för att på bästa sätt kunna bidra till en god rapportering. Bland annat talas det om huruvida ett formulär ska bygga på fritext eller bestå av standardiserade frågor.

En nackdel med fritextfrågor är att de är mycket svåra att standardisera samt att kvalitén på avvikelserapporterna kan vara väldigt varierande. För att förenkla för dem som skall fylla i en blankett/rapport kan en förutbestämd ordlista bifogas. Det kan medföra en viss standardisering av formuläret. [JOH00]

2.3 Knowledge management

Detta teorikapitel kommer att behandla området *knowledge management*, eller kunskapshantering som är den svenska benämningen. Avsnittet innehåller teori om kunskapshantering, attityder, kunskapsdelning med mera.

2.3.1 Vad är knowledge management?

Målet med kunskapshantering kan sägas vara att fånga, lagra och tillhandahålla användbar kunskap på ett enkelt sätt för att vem som helst som behöver den ska kunna komma åt kunskapen varsomhelst och när som helst. Knowledge management handlar om att företag och organisationer på ett medvetet sätt jobbar med kunskapshantering.

Awad och Ghaziri (2004) nämner i sin bok ”knowledge management” några myter som finns om kunskapshantering. En av dessa är att kunskapshantering bara fungerar *inom* organisationer. De är beredda att hålla med i det påståendet i vissa situationer men de poängterar att den mest värdefulla kunskapen i en organisation kommer utifrån. Problem med extern kunskapshantering är som författarna ser det; teknologi, säkerhetsfrågor och komplex design på sådana system.

2.3.2 Kunskapsdelning

Kunskapsdelning är den mest centrala delen i kunskapshantering. Kunskapsdelning kan förklaras med följande mening: ”ett systematiskt infångande av kunskap från forskning och erfarenheter, organisering och lagring av information för lätt åtkomst, överföring och delning mellan intressenter i ett tvåvägsutbyte”. [WOR05]

Fördelar med kunskapsdelning är att man kan förhindra att man i en verksamhet måste börja från ”scratch” när exempelvis ett projekt ska genomföras och på så sätt spara tid och pengar.

Kunskapsdelning är dock inte gjord i en handvändning. Boone (1997) menar att kunskapsdelning ofta är en kaotisk oordnad process där medarbetarnas syn på kunskap, kunskapens värde och användningsområde påverkar processen att dela men också själva skapandet av kunskap.

De två rollerna, ”den som tar emot” och ”den som ger” är tätt sammankopplade (Dixon, 2000). Stewart (1999) betonar också att kunskapsgenerering och kunskapsdelning bygger på varandra. Ny kunskap genereras genom att den skapas och upptäcks och kunskap delas genom att gammal kunskap återanvänds, förpackas och appliceras i nya sammanhang eller sprids genom dialog i vilken kunskap också uppstår. För att en dialog ska äga rum är det viktigt att det finns ett gemensamt språk, ett behov och en gemensam mening med det som diskuteras. [HÅK03]

Kunskapsdelning är också den del av kunskapshantering som är den mest problematiska i många sammanhang. Att dela med sig av sin hårt vunna kunskap är för många människor och organisationer inte helt enkelt eftersom kunskap ofta är ett konkurrensmedel.

Det finns även en del andra begränsande faktorer för kunskapsdelning, Awad och Ghaziri [AWA04] nämner följande:

- *Brist på förtroende*. Att två kommunicerande parter litar på varandra är en förutsättning för att ett meningsfullt kunskapsutbyte ska kunna ske. Kultur, språk och status kan bidra till antingen ökat eller minskat förtroende för den andra parten.

- *Tidsbrist.* Människor tenderar att hitta kunskap på det närmsta och hos det enklaste stället, inte på det bästa stället. För att expediera kunskapsdelning måste de inblandade människorna visa intresse och ta sig tid att hitta platser där informationsutbytet kan ske på bästa sätt.

- *Status hos kunskapsbäraren.* Människor tenderar att ta till sig information olika beroende på vem som ger dem den. Ju högre status en människa eller organisation har desto lättare är det för mottagaren att ta till sig och sätta värde på informationen.

- *Kvalitet och hastighet hos överföringen.* När kunskap är förmedlad från en pålitlig källa är den förväntad att vara av god kvalitet. Även tiden till dess att kunskapen kommer till användning är viktig för att man ska se någon nytta med den.

I litteraturen diskuteras det ofta huruvida rollen och värdet av datorbaserade system för kunskapshantering bör starta med teknologi eller med mänskliga sociala processer. Malhotra (2000) menar att det i första hand bör koncentreras på utveckling och implementering av IT-stöd för kunskapshantering och

kunskapsdelning. Därefter bör det fokuseras på att skapa en vision och kultur som motiverar till kunskapsdelning mellan individer i företaget. I och med att IT-stödet redan implementerat antas det bli lättare för individerna att börja använda dem vart eftersom de anammar den nya kunskapsvisionen. I motsatts till detta säger Walsham (2001) att kommunikations- och informationsteknologin inte är lösningen på förbättrad kunskapsdelning mellan individer inom företag. Istället måste kunskapshanteringsaktiviteterna först och främst börja med sociala processer mellan människorna inom företaget. Kunskapshanteringssystem kan inte ersätta behovet av mänskliga relationer och det är avgörande att människor inom företaget inser vikten av att dela med sig av sin kunskap och kompetens från första början innan tekniska aspekter eventuellt får komma in i bilden. [HÅK03]

3 Metod

I det här kapitlet beskriver jag på vilket sätt jag har arbetat med uppsatsen och vilka vetenskapliga ansatser jag har använt mig av. Alltifrån inledande litteraturstudier till diskussion och resultat av det analyserade data.

3.1 Forskningsmetoder

De forskningsmetoder jag kommer att använda mig av för att komma till ett resultat är litteraturstudier och en fallstudie.

För att sätta mig in i ämnet har jag till att börja med läst ur böcker, uppsatser och artiklar som jag har hittat på biblioteket och på Internet. Jag har sedan skrivit ner den teori och de begrepp som jag tycker utgör en grund för min avgränsade del inom incidenthantering. Med hjälp av teorin och empirin har jag slutligen besvarat forskningsfrågan.

3.1.1 Deduktiv eller induktiv

Deduktiv eller induktiv ansats handlar om huruvida man utgår från teorier i sitt arbete eller skapar egna teorier. Deduktiv ansats handlar om att bevisa befintliga teorier. Forskaren har en klar bild över området han undersöker. Induktiva teorier handlar om att göra undersökningar i verkligheten utan att först ha förankrat det i befintlig teori. Detta medför att forskaren skapar teori utifrån en empirisk undersökning.

Eftersom det finns relevanta torier inom mitt område har jag valt det deduktiva angreppssättet. Jag kommer alltså att dra deduktiva slutsatser när jag jämför mina insamlade data med befintlig teori.

3.1.2 Kvalitativ och kvantitativ ansats

En vanlig indelning vad gäller forskningsmetoder är kvalitativ och kvantitativ forskning. Patel och Davidson säger att syftet med dessa två synsätt är att berätta på vilket sätt analysen av det insamlade data kommer att ske.

Den kvantitativa ansatsen innebär att forskarna använder sig av statistiska analysmetoder när de analyserar det insamlade data. Den insamlade data är med andra ord mätbar och tilldelad numeriska värden. En kvalitativ ansats innebär däremot analysmetoder som är av en verbal och diskuterande karaktär. Kvalitativ forskning försöker förklara olika fenomen genom diskussion. [PAT03]

Mina intentioner är att skriva en uppsats med en kvalitativ inriktning. Jag vill skriva uppsatsen med en diskuterande ansats eftersom jag inte väntar att få enkla och mätbara svar på mina frågor. Ofta presenteras kvalitativ och tolkande forskning som en kontrast till ”traditionell” naturvetenskaplig forskning.

I samhällsvetenskap bör forskaren hålla sig borta från en strikt orsaksbestämd determinism i förklaringar, eftersom det ofta är fråga om påverkande faktorer, så kallat ”mjukt” orsaksförhållande.

3.2 Undersökningsansats

Undersökningen kommer att göras i form av en fallstudie. En fallstudie är enligt Patel och Davidson en undersökning som forskaren gör på en liten grupp. De säger också att en fallstudie är lämplig att göra när man ställer frågor av typen ”hur” och ”varför”, vilka är frågor som jag ställer i denna uppsats. Andra alternativa undersökningssätt som författarna nämner är exempelvis experiment och survey (undersökning på en större grupp).

Patel och Davidson nämner också olika insamlingstekniker som finns att tillgå i en fallstudie. Dessa kan vara dokumentstudier, testning, enkäter, observationer och intervjuer. De påstår inte att någon är bättre än någon annan utan att valet av teknik är beroende på frågeställning och situation. [PAT03]

3.3 Fallstudien

En fallstudie har gjorts på ett antal organisationer i Luleå. Min ansats har varit att göra fallstudierna på relativt stora företag som är beroende av fungerande informationssystem för organisationens dagliga verksamhet och där en ickefungerande informationsteknik leder till ett verksamhetskritiskt tillstånd. I detta avsnitt kommer jag att beskriva hur valet av fallstudieobjekt gått till och beskriva de forskningsmetoder som används i fallstudien.

3.3.1 Val av fallstudieobjekt

Fallstudier har gjorts både på statliga och kommunala organisationer och privata företag, eftersom jag tror att det kan finnas viktiga skillnader i synsätt inom det område som den här uppsatsen behandlar.

Viljan och resurserna att rapportera incidenter externt skiljer sig mellan statliga myndigheter och privata företag. Därför är det intressant att undersöka dessa olika typer av organisationer.

3.3.2 Datainsamlingsmetod

Kvalitativ empiri kan bedrivas på många olika sätt. Jag har valt att genomföra datainsamlingen i form av intervjuer med berörda personer. Intervjuerna kommer att vara semistrukturerade, vilket innebär att det kommer att finnas utrymme för diskussion. Jag tror nämligen att många svar kräver diskussioner genom vilka jag

kan få en djupare förståelse för olika strategier olika verksamheter använder sig av.

Det hade funnits möjligheter att även genomföra datainsamlingen med hjälp av enkäter, men eftersom jag har en kvalitativ ansats är det lättare att få fram relevanta svar genom en diskussion.

Intervjuer

Jag ska genomföra fallstudien i form av kvalitativa intervjuer där jag ska ställa semistrukturerade och relativt standardiserade frågor.

Frågornas grad av strukturering handlar om hur pass begränsad respondenten är i sina svar. Vid helt strukturerade frågor kan personen i princip svara ja eller nej. Graden av standardisering handlar om huruvida man följer en frågemall med färdiga frågor eller om man genomför intervjun i form av en diskussion. [PAT03]

Eftersom jag vill jämföra de olika svaren jag får kommer jag att använda mig av relativt standardiserade frågor. Detta möjliggör ändå att jag kan ställa följdfrågor för att förtydliga svaren.

Intervjuerna kommer att genomföras både traditionellt där jag möter personen ifråga, men kan i vissa fall behöva genomföras via telefon.

3.3.3 Val av respondenter

Jag har valt att intervjua sådana personer som har ansvar för incidentrapportering i sin organisation. Om en sådan saknas kommer jag att intervjua den person som jag, efter att jag har talat med personer hos den aktuella organisationen, tycker ligger närmast en sådan roll. Min avsikt är att intervjua liknande personer hos samtliga organisationer. Detta för att få svar som går att jämföra på ett så rättvisande sätt som möjligt.

3.4 Analysmetod

Patel och Davidson skriver att ambitionen i kvalitativ forskning är att försöka förstå och analysera helheter. Detta åstadkommer jag i form av diskuterande avsnitt där jag under olika rubriker diskuterar hur respondenterna ser på att använda sig av ett nationellt incidenthanteringscentra. De ovanstående författarna säger också att det inte finns några enkla procedurer och rutiner att följa vid kvalitativ bearbetning. Varje kvalitativ forskning kräver sin unika variant. [PAT03]

3.5 Validitet och reliabilitet

Begreppen validitet och reliabilitet handlar om hur tillförlitlig och giltig en undersökning är.

Validitet är huruvida forskaren undersöker rätt saker. Är svaren relevanta för forskningsfrågan? För att öka validiteten i undersökningen kan man enligt Yin, 1994, inhämta data på flera olika sätt, exempelvis genom att samla in data både i form av intervjuer och i forma av dokumentstudier.

Reliabiliteten, alltså tillförlitligheten säger huruvida en undersökning skulle få samma resultat om den genomfördes vid ett senare tillfälle med samma förutsättningar. Med andra ord svarar den på frågan om forskaren mäter på rätt sätt. Begreppet reliabilitet brukar dock sällan användas när man pratar om kvalitativ forskning. Patel och Davidson menar exempelvis att man vid två likadana intervjuer med samma person kan få skillnader i svaren utan att intervjuaren nödvändigtvis måste ha begått något fel. [PAT03]

4 Empiri

Här kommer en presentation av resultatet av de fallstudier jag har gjort hos fyra olika organisationer. Förutom Sitic kallar jag dem Universitet A, Företag B, Kommun C och Myndighet D. Intervjuerna hos de olika organisationerna kommer att presenteras var för sig med en kort inledning där jag förklarar hur och med vem intervjun genomfördes. Där så krävs, finns en kort presentation av organisationens verksamhet.

4.1 Sitic

Jag har varit i kontakt med Sitic via e-post och telefon. Jag ställde några frågor i brevet som jag följde upp med en telefonintervju. Jag har även besökt deras hemsida där jag har tagit del av den information som följer.

Sitic är en svensk CERT-organisation och har ett fyrdelat uppdrag som består av följande delar:

- Inrätta ett system för informationsutbyte mellan samhällets organisationer
- Sammanställa och ge ut statistik
- Snabbt informera om nya hot
- Lämna information och råd om förebyggande åtgärder

I Sitics dagliga arbete ingår traditionell omvärldsbevakning, att inhämta information från en stor mängd källor. Denna information analyseras och om den bedöms vara relevant för Sitics intressenter så paketeras den och ges ut i särskilda råd, eller om omständigheterna kräver det, i blixtmeddelanden. Sitic har även samarbete med andra CERT:ar, exempelvis SUNETs, för att ta åt sig och dela med sig av incidentinformation.

Sitic har labbresurser som används kontinuerligt för att genomföra olika tester på programvaror, hårdvaror, konfigurationer och system. Denna verksamhet kan verifiera inhämtad information och kan också leda till att nya IT-säkerhetsproblem upptäcks.

På hemsidan kan man också läsa att viktigaste är att rapporter kommer in och inte i vilken form de kommer in. Det finns med andra ord få obligatoriska uppgifter man måste uppge vid en inrapportering. [SIT05]

Sitic har fått kritik för bland annat långsam reaktion på hot som har uppkommit samt. Detta delvis bero på att Sitic bara är bemannat på kontorstid vilket gör att en incident som uppstår på kvällen kan vidareförmedlas till samhället föst dagen därpå. Sitic funderar på grund av detta att införa jourverksamhet. En annan orsak till att de har upplevts som långsamma är att de när de får reda på nya hot (oftast från utlandet) måste översätta dessa till svenska.

Sitic går även ut med färre varningar än dess motsvarighet i exempelvis USA. Detta beror på att Sitics rutiner när de får in rapporter ser annorlunda ut än

motsvarigheterna utomlands. Medan utländska Computer Emergency Response Team, Cert-funktioner, lägger ut flera varningar per dag lägger Sitic endast ut varningar av två anledningar. Det första kravet är att det finns stor risk för spridning. Det andra kravet är att hotet ska röra en produkt som är allmänt spridd bland myndigheterna.

4.1.1 Intervjuresultat

Följande svar fick jag på frågor som jag ställt via e-post och där frågat vad de låga rapporteringstalen berodde på och om det fortfarande var ett problem, jag frågade även till vem Sitic riktar sin verksamhet till.

När vi startade upp Sitic i januari 2003 kunde vi endast stödja oss på 2 kap 2 § (försvarssekretess)i Sekretesslagen för att kunna sekretessbelägga incidentrapporter. Detta innebar att endast de organisationer som omfattas av försvarssekretess, ca 31 myndigheter, kunde rapportera utan risk för att rapporterna kunde lämnas ut. Detta innebar att endast en mycket liten del av samhällets organisationer rapporterade till oss. Vi lämnar inte ut hur många rapporter vi får in. Den 1 juli 2004 ändrades Sekretesslagen så att vi nu har fått en förändring i 5 kap 2 § Sekretesslagen som medför att all information som har att göra med säkerhetsåtgärder i IT-system kan sekretessbeläggas. Nu kan alltså även näringsliv rapportera till oss utan risk för att deras rapporter kan lämnas ut. Sedan ändringen trädde i kraft har vi fått rapporter från näringslivet.

Skälet till att organisationer inte rapporterar är olika, en del organisationer kanske inte har verktyg för att upptäcka incidenter, andra kanske inte har rutiner för att rapportera incidenter till säkerhetsansvarig befattningshavare, en del ser inga skäl till att rapportera till Sitic av en rad orsaker som vi tänkte genomföra en mörkertalsstudie om nu under våren.

Våra argument för att man ska incidentrapportera är följande:

-Varje enskild rapport ökar möjligheterna att generera relevant statistik och hotbildsrapportering – beslutsunderlag

-Uppnå kostnadsreduktioner genom samarbete

-Inrapportering kommer andra tillgodo (kan vara först att upptäcka en ny företeelse)

-Sitic kan eventuellt associera en inkommen rapport med en eller flera andra (se mönster i hot och angrepp)

-Sitic kan förfoga över (ännu inte) allmänt känd information

-Varje enskild rapport ökar möjligheterna att generera relevanta råd, rekommendationer och andra dokument

-Sitic kan, i särskilt intressanta fall, bidra med spetskompetens, egen såväl som samarbetspartners, i arbetet med analys av händelsen.

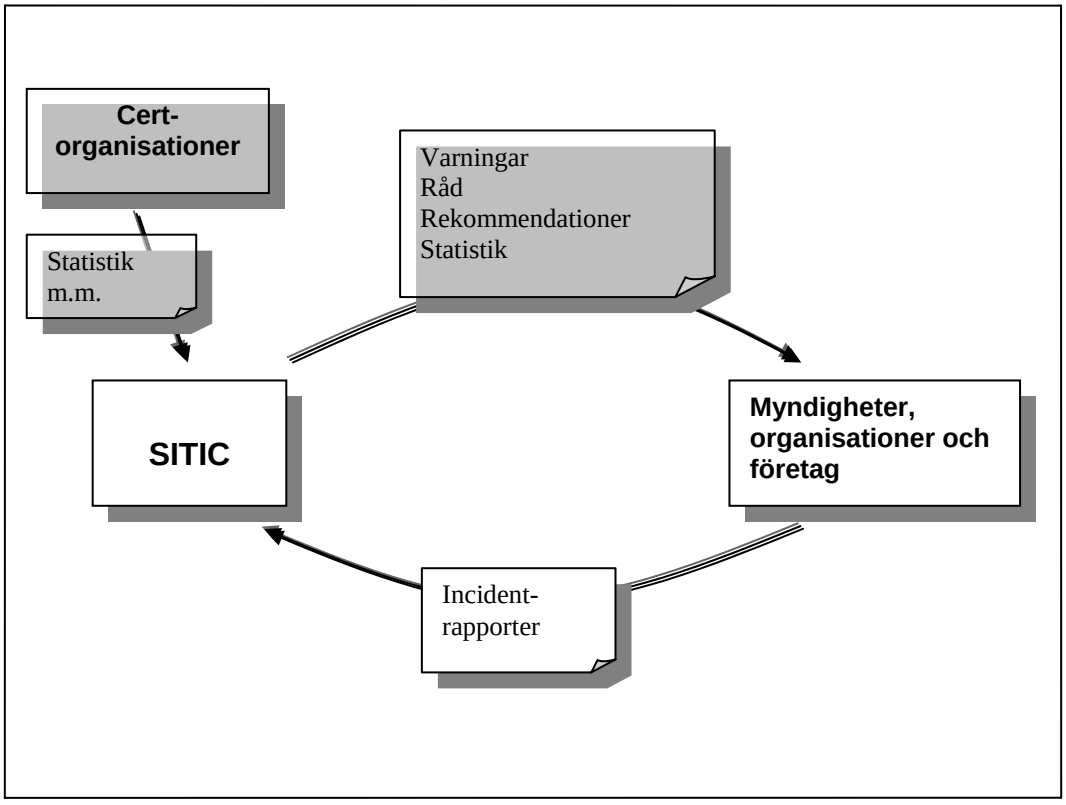
Jag har även genomfört en intervju via telefon där jag fick den ytterligare informationen som följer nedan.

Jag har talat med en av de ansvarige på Sitic och frågade en del kring olika problem som jag upplever att finnas i deras arbete. De medgav att det inte hade kommit in speciellt många rapporter, men att en viss ökning hade skett. Om huruvida den ökningen berodde på den omtalade lagändringen eller för att de nyligen hade ändrat gränssnittet på inrapporteringsformuläret kunde han inte säga eftersom dessa förändringar skett ungefär samtidigt.

Att företag rapporterar är nödvändigt för att Sitic ska kunna varna för olika hot, men däremot får de sina statistikrapporter från annat håll.

Jag frågade även om hur deras marknadsföring ser ut. Han svarade att de inte har marknadsfört sig i någon större omfattning. Den utåtriktade verksamheten de bedrivit hittills är att de medverkat i olika konferenser.

De sa vidare att de inte tagit några beslut om hur de ska gå vidare i arbetet med exempelvis näringslivet.



Figur 4.1 Sitics funktion och samarbete

4.2 Universitet A

Den första intervjun genomfördes på ett universitet. Universitetet har en omfattande datoranvändning och har en utsatt miljö exempelvis på grund av att många användare använder olika applikationer och operativsystem. Därför anser jag att ett universitet är en lämplig respondent i den här typen av undersökning.

4.2.1 Intervjuresultat

På detta universitet intervjuade jag en datorsäkerhetsansvarig som också är ansvarig för rapportering av IT-incidenter. Han sa att han både tar emot incidentanmälningar och skickar iväg anmälningar angående sådant som universitetet drabbas av.

Han sa vidare att de på universitetet i första hand rapporterar till SUNET:s CERT som är Sveriges universitets och högskolors gemensamma CERT. Personen visste också att SUNET har ett visst samarbete med Sitic, han tror att de rapporterar sinsemellan. Han ansåg därför inte att det var aktuellt att universiteten rapporterade direkt till Sitic. Uuniversitetet har också haft någon enstaka informationsträff med Sitic där Sitic informerat om sitt arbete.

Alla portscanningar som universitetet utsätts för rapporteras automatiskt till SUNET. Universitetet rapporterar inte något regelbundet, om det inte är för några speciella händelser eller incidenter som har inträffat.

Personen anser att det är bra att det finns en generell organisation, som Sitic, för hela landet som kan hantera olika hot och incidenter. Han tror att den skulle fungera bra om man skulle kunna lösa problemet med att alla inte vill rapportera. Han anser att SUNET-CERT:en fungerar bra, att de blir hjälpta av samarbetet och att den innehåller de delar som den bör för att uppfylla sitt syfte.

Han såg inga hinder med att dela med sig av säkerhetsinformation. Eftersom han ser universitet som statliga myndigheter eller institutioner, men han sade att det problemet troligtvis finns hos företag som sysslar med affärer där incidentrapportering kan medföra så kallad ”bad will”.

På frågan om hur han ställer sig till en eventuell skyldighet att rapportera IT-incidenter nämner han den arbetsbörda man lägger på verksamheterna och säger att det tar mycket tid att sammanställa rapporter och att organisationer kanske inte kan räkna hem de pengar som läggs ned.

Han säger också att olika organisationer inte vill rapportera allt de drabbas av och att de därför mörkar och säger: ”det där har vi aldrig sett”.

Han nämnde också att den lagändring som trätt i kraft möjligen kan göra det mer intressant för myndigheter och företag att rapportera.

Universitetet har inte något internt incidentrapporteringssystem. Den grupp som är säkerhetsansvariga får kännedom om att incidenter inträffat via informella mail

eller samtal från personalen samt via automatlarm. I universitets policy står det att anställda skall rapportera incidenter till ansvariga för IT-säkerheten. Portscanningar rapporteras automatiskt till SUNET eftersom de är nätägare och kan jämfört med exempelvis Sitic enklare kräva att teknik finns installerad hos olika universitet för att de ska kunna övervaka nättrafiken.

4.3 Företag B

Företag B är ett IT-företag vars verksamhet omfattar konsulttjänster och produktutveckling. Tjänsterna går ut på att förbättra stora organisationers inköpsverksamheter

Intervjun med Företag B genomfördes via telefon med en IT-ansvarig på företaget.

4.3.1 Intervjuresultat

Personen på Företag B kände vid intervjutillfället inte till Sitic. Han arbetade på ett relativt litet företag och anser därför inte att incidentrapportering gällde dem. Han inte såg det ekonomiskt försvarbart när de kan åtgärda sina säkerhetsproblem själva.

Den incidenthantering företaget har idag går till stort ut på att leta efter hot på olika abuse-adresser och kontrollerar vilka som exempelvis portscannar dem. De har inget samarbete med något annat företag vad gäller IT-säkerheten.

Personen säger dock att de mycket väl skulle kunna tänka sig att rapportera till Sitic så länge det inte skulle medföra kostnader för dem. Han anser att det inte är aktuellt eftersom de inte har haft några problem hittills. Eftersom de har sin information skyddad så anser de inte att det finns något att plocka och därför är de inte någon målgrupp för ”hackers” med flera.

Han ser inga hinder med att dela med sig av incidentinformation så länge det inte handlar om intern information. Exempelvis IP-nummer av vilka de blir portscannade av ser han inga problem att dela med sig av.

Han betonade att anledningen till att de inte rapporterar några incidenter är att de inte har några sådana och därför inte ser någon nytta med det. Han medger dock att de säkert hade tänkt i andra banor om de ofta hade utsatts för incidenter av något slag.

Angående en eventuell skyldighet att rapportera incidenter säger han att de naturligtvis hade gjort det, men att de inte hade varit så glada om det medförde ett merjobb för dem.

Företaget har inte några formella rutiner för incidenthantering. De anser sig ha kompetensen att själv åtgärda de problem som uppstår

4.4 Kommun C

Intervjun med Kommun C skedde via telefon. Jag intervjuade en IT-chef hos organisationen.

4.4.1 Intervjuresultat

Kommun C brukar inte rapportera eller ta del av incidentinformation till eller från någon extern CERT-organisation. De har däremot en samordning med kommunförbundet som bevakar incidenter för kommunernas räkning. IT-chefen sa att de dock har ett visst samarbete med några externa företag som går ut med varningar kring kritiska säkerhetshål i olika typer av system som kommunen har samt virusvarningar med mera. De prenumererar på tjänster från företag som går ut med varningar och rekommendationer, så kallade ”alerts” som säger att nu är det här och det här på gång.

Han kunde inte till en början påminna sig om att han ens hade hört talas om Sitic. Men kom sedan på att det nyligen hade varit uppe en fråga angående rapportering till Sitic, men att det inte hade kommit några riktlinjer från exempelvis kommunförbundet om hur de skulle gå vidare med frågan. Han ansåg att Sitic skulle fylla en roll som en samordnande myndighet i IT-säkerhetsfrågor.

Den rapportering som sker i dagsläget hos kommunen sker i första hand internt till kommunledning, tjänstemän och politiker.

Han ansåg inte att de hade några incidenter i dagsläget som skulle vara av nationellt intresse. Han såg dock inte något hinder med att rapportera, inte heller om det skulle komma en lag som tvingar dem att rapportera, annat än att om rapporterna skulle bli offentliga. Han sa att rapportering av incidenter skulle kunna röja information om säkerhetsluckor som man inte gärna vill dela med sig av.

Han gav även förslag på hur Sitic borde utforma sitt rapporteringssystem. Han sa att det först och främst bör vara ett enkelt system, det är en oerhörd mängd saker man som säkerhetsansvarig ska bevaka och en sådan person har inte den tiden det innebär att leta på nätet efter, hot som kan påverka just mina system och applikationer och filtrera bort onödig information.

Det skulle vara bra om man kunde prenumerera på tjänster av Sitic som gäller de hot som vi specifikt kan drabbas av. Som det är idag är det så att hoten som de varnar för är generella och därför innehåller information som vi på kommunen inte har användning av exempelvis luckor i system som vi inte har i vår organisation.

Själva inrapporteringen bör fungera i form av ett webbgränssnitt där det finns bra metadata och färdiga kategorier så att man snabbt kan hamna i rätt fack direkt, vilket hjälper till att man också får relevant information tillbaka.

4.5 Myndighet D

Jag har pratat med den informationssäkerhetsansvarige på Myndighet D som är en av de 31 myndigheter och verk som Sitic i ett inledande skede har riktat sin verksamhet mot.

4.5.1 Intervjuresultat

Myndighet har inte rapporterat till Sitic än så länge, de anser inte att de haft några incidenter som bör rapporteras, de håller sig däremot uppdaterade med information från Sitic angående hot och risker, men det gör de också från andra ställen.

Angående synen på en nationell IT-incidenthanteringsorganisation så hade respondenten iakttagit Sitics tillkomst men inte varit särskilt imponerad. Han anser att det är svårt att skapa en sådan företeelse som får en relevant snabbhet, den organisationen blir inte tillräckligt smidig. Det var i början meningen att Sitic skulle vara en alert reaktiv funktion för olika hotbilder i Sverige, men det trodde han skulle bli svårt att genomföra i praktiken. Han trodde dock att den mycket väl skulle kunna fylla en uppgift i uppföljningssyfte.

Den incidentinformation de finner hos Sitic kan de hitta på andra ställen mycket snabbare. Han nämnde att Sitic i och för sig ibland har panikutskick där det går snabbare, men i det hela taget går det för långsamt. Den talande faktorn för dagens hot mot IT-verksamheter är hotens snabbhet. Att det då skulle finnas en organisation som skulle kunna möta alla dessa hot på ett tillfredsställande sätt och tillräckligt snabbt trodde han var svårt.

De skulle mycket väl kunna tänka sig att rapportera till Sitic när de drabbas av incidenter. Personen såg en nytta med den typen av organisationer genom att man kan dra nytta av andras erfarenheter.

Han ansåg inte att det är ett behov om att lagstifta om att man måste rapportera, i sådana fall är det något e-nämnden ska besluta om men något sådant har han inte sett och han tror inte heller att det kommer att bli så.

Han sa också att han önskade ville ha ett system där all personal i hans lokalkontor skulle kunna använda för att rapportera i. Han ansåg att ett sådant system och rutiner idag saknades på hans myndighet Det tänkta systemet ansåg han skulle kunna fungera på så sätt att varje anställd har en ikon på sitt skrivbord på datorn och kan rapportera incidenter som sedan kontrolleras av någon ansvarig hos tullen, kontrollen kan innebära att personinformation plockas bort innan den skickas iväg till någon extern organisation. Han tror att man på så sätt skulle få en effektivare incidentrapportering där varje anställd direkt kan rapportera incidenter.

	Universitet A	**Företag B**	**Kommun C**	**Myndighet D**
Känner ni till Sitic?	Ja	Nej	Nej	Ja
Har ni samarbete med någon extern org.?	Ja (SUNET)	Nej, men tittar på varnings-siter	Ja	Ja, Sitic bl.a.
Skulle ni kunna tänka er att rapportera till Sitic?	Tror inte det	Ja, om behov uppstår	Ja, kanske	Ja
Finns det fördelar med en nationell org.?	Ja	Ja	Ja	Ja
Vad tycker ni om en eventuell rapporterings-skyldighet?	Tveksamt, mycket arbetsbörda leder till ovilja	Nja, mycket arbetsbörda. Hade nog inte varit så glada	JA, om man löser problemen med offentlighet	Tveksam
Hur bör ett rapporteringssystem se ut?	-	-	Lättanvänt och anpassnings bart för våra behov	Lättåtkomligt för all personal

Tabell 1. Matris över utvalda frågor och svar

5 Analys

I det här kapitlet kommer jag att analysera de intervjuer jag har gjort. Jag kommer att sammanställa och jämföra de olika svaren under olika rubriker för att jag på så sätt ska kunna dra slutsatser utifrån det. Vissa av frågorna jag ställde under intervjun kommer att fungera som rubriker i detta analyskapitel.

5.1 Genomförs det någon extern rapportering av IT-incidenter hos er?

Allen nämner (se avsnitt 2.2.2) vikten av att informera andra organisationer om incidenter. Säkerhetsorganisationer i olika företag kan då arbeta förebyggande genom att ta del av andras incidenter. Allen föreslår därför att incidenter även skall rapporteras till någon organisation som arbetar med att förmedla denna information.

Vad jag har kunnat se i min undersökning, så har alla organisationer någon sorts incidenthantering där de tar emot incidentinformation i form av varningar och råd. Det är dock inte många organisationer som rapporterar IT-incidenter till någon större oberoende incidenthanteringsorganisation. Det finns som jag ser det olika anledningar till detta. Vissa organisationer i min undersökning påstod sig vara för små och därför inte villiga satsa tid på att rapportera sina incidenter. Andra organisationer använde sig av IT-säkerhetsföretag, vilka de prenumererade på olika tjänster av. En annan sak är att organisationer inte ser att rapporteringen gagnar dem själva och därför inte anser det lönt att rapportera. Exempelvis ansåg sig inte det företag jag har intervjuat ha några större säkerhetsproblem och såg därför inte nyttan med att rapportera, men skulle om de utsattes för flera incidenter troligen ändra sin inställning.

Universitetet rapporterar och använder sig av SUNET:s CERT. De ”rapporterar” delvis genom automatiska kontroller som SUNET gör centralt. Om speciella incidenter inträffar så rapporteras dessa till SUNET.

Myndigheten och kommunen kände visserligen till Sitic, men hade inte rapporterat dit. De tar del av varningar som Sitic utfärdar, men får också varningar från andra ställen.

5.2 Känner ni till Sitic?

Av de organisationer jag har varit kontakt med kände tre stycken till Sitic. Jag ställde frågor om detta till Sitic och de svarade att de i ett inledande skede, före sekretesslagändringen, enbart riktade in sig på ett antal organisationer och myndigheter (31 stycken) som kunde garanteras sekretess tack vare lagen om försvarssekretess. Sitic har därför under det första året riktat sin marknadsföring mot dessa organisationer, vilket kan förklara en del av den bristfälliga inrapporteringen och det faktum att så få organisationer känner till dem.

Sitic nämnde att de inte har genomfört någon marknadsföring utan endast deltagit vid seminarier. I vissa fall har de riktat sig mot enskilda organisationer exempelvis Stockholms läns landsting.

5.3 Vilka fördelar och nackdelar finns det med en nationell oberoende incidenthanteringsorganisation?

I avsnitt 2.2.2 nämns tre olika syften med rapportering till externa organisationer. De flesta respondenterna tyckte att syftena med en nationell och generell incidenthanteringsorganisation är positiva. Det vill säga att en nationell säkerhetsorganisation bör finnas och ha en samordnande roll i samhället.

Det negativa som personen på Myndigheten såg med detta är det faktum att hoten och attackerna framförallt har ökat i snabbhet. Han ansåg därför att det är svårt för en stor incidenthanteringsorganisation att vara tillräckligt snabb för att man ska ha någon nytta av de varningar och råd de går ut med. Denna person ansåg emellertid att en sådan organisation skulle fylla en roll i uppföljningssyfte. Awad och Ghaziri nämner i 2.3.2 att kvalité och hastighet i överföringen är viktigt i ett förhållande av den här typen.

Organisationerna ansåg alla att de ofta kunde få bättre säkerhetsinformation från andra källor som är mer anpassade för de specifika incidenter som berörde just deras applikationer och datorprogram.

5.4 Hur ser ni på en eventuell skyldighet att rapportera era IT-incidenter?

Angående hypotesen att bli tvingad att rapportera IT-incidenter var åsikterna relativt lika hos alla organisationer. Ingen av respondenterna såg någon avgörande fördel med detta

Personen på universitetet sa att man då lägger en för stor arbetsbörda på organisationer och att de sannolikt inte ser att de kan räkna hem dessa utgifter. Som en reaktion på det kan det hända att de mörkar och säger att ”det där har vi aldrig sett”. Även Företaget befarar att det skulle bli merjobb. Eftersom de är ett litet privat företag som löser sina problem varefter de uppkommer så tycker de att det skulle kännas meningslöst. Myndigheten anser inte att det finns ett behov om att lagstifta om att man måste rapportera, i sådana fall är det något e-nämnden ska besluta om, men något sådant har han inte sett och han tror inte heller att det kommer att bli så.

Kommunen ser inget hinder i det förutom att det att rapporterna blir offentliga och man på så sätt röjer sina eventuella brister och säkerhetshål.

5.5 Analys genom Knowledge management

Här kommer jag att analysera Sitics verksamhet och samarbetet med de andra respondenternas samarbete utifrån Awad och Ghaziris bok ”knowledge management”, se kapitel 2.3.

5.5.1 Förtroende

För att två parter på ett acceptabelt sätt ska kunna kommunicera och dela med sig av kunskap krävs det att parterna litar på varandra och att de talar ”samma språk”. I det fallet jag har undersökt har jag märkt att det hos vissa inte finns något speciellt stort förtroende för Sitic som incidenthanteringsorganisation. Många ser den som en långsam organisation som inte kommer ut med incidentvarningar i tid. Detta gör att många inte ser något mervärde i att rapportera dit.

Universitetet och kommunen hade båda förtroende för Sitic, men på grund av att Universitetet hade samarbete med SUNET och Kommunen väntade på riktlinjer från kommunförbundet så hade de idag inte något mer ingående samarbete.

Företaget kände inte till Sitic, men såg ändå relativt positivt på en sådan organisation existerade.

Myndigheten hade inget stort förtroende för Sitic. Respondenten hade iakttagit Sitics tillkomst och utveckling men var inte imponerad. Han anser att det är svårt att skapa en sådan företeelse som får en relevant snabbhet, den organisationen blir inte tillräckligt smidig. Det var i början meningen att Sitic skulle vara en alert reaktiv funktion för olika hotbilder i Sverige, men det trodde han skulle bli svårt att genomföra i praktiken. Han trodde dock att den mycket väl skulle kunna fylla en uppgift i uppföljningssyfte.

5.5.2 Tidsbrist

Författarna nämner att människor tenderar att hitta kunskap på det närmsta och hos det enklaste stället, inte på det bästa stället. För att expediera kunskapsdelning måste de inblandade människorna visa intresse och ta sig tid att hitta platser där informationsutbytet kan ske på bästa sätt.

Ett ständigt återkommande problem med att rapportera incidenter är tidsbrist. Många av respondenterna svarade att de inte har tid att rapportera och att det endast skulle vara värt att göra detta om de har akuta problem som i en förlängning skulle kunna leda till förluster.

Denna tidsbrist som Awad och Ghaziri nämner skulle enligt kommunen kunna åtgärdas genom att Sitic skulle skräddarsy sin verksamhet för olika ”kunder”. Respondenten ansåg att det tar för mycket tid att analysera de hot som Sitic går ut med då den informationen ofta är sådant som kommunen inte har användning för.

För företaget är tid och pengar kritiska resurser och ett krav av dem för att rapportera är att rapporteringen inte kostar pengar eller blir merjobb för dem.

Samtliga respondenter som ingår i undersökningen hade samarbeten med företag som i många fall också var leverantörer av de den programvaran som de använde. Detta gör att organisationerna kan ta del av incidentinformation på ett snabbare och effektivare sätt.

5.5.3 Kvalitet och hastigheten i överföringen

Awad och Ghaziri säger att snabbheten och kvaliteten hos den information som förmedlas i ett kunskapsdelningsförhållande är mycket viktig. Några av respondenterna som jag har varit i kontakt med nämner brister i både kvalitet och snabbhet. Exempelvis är den information de tar emot inte alltid tillämpbar i deras organisation eller så kommer den för sent och kan därför inte användas.

Kommunen nämner att de varningar som Sitic går ut med bör vara mer specifika för just deras problem, annars riskerar de att överhopas med en mängd information som de inte har någon nytta av. Myndigheten tycker att Sitic är för stor och omständig med för mycket byråkrati för att kunna varna för nya hot i tid. Förtroendet för, i det här fallet, Sitic är beroende på hur snabbt och hur bra de agerar när en organisation kontaktar dem.

Allen nämner i 2.2.4 att en snabb inrapporteringsrutin är viktig. Respondenten hos myndigheten efterlyser rutiner hos sin organisation där samtliga anställda på ett snabbt och enkelt sätt kan rapportera från sina egna datorer direkt när de upptäcker incidenter. Detta tror respondenten skulle snabba på rapporteringen och försäkra att rapporter kommer de ansvariga till kännedom.

5.6 Incidentrapporteringssystem

Systemet vilket organisationerna ska använda för att rapportera incidenter och ta emot incidentinformation är värt att analyseras.

Awad och Ghaziri nämner vikten av användarmedverkan vid framtagning av ett kunskapshanteringssystem. De säger att systemet bör utvecklas precis som andra informationssystem i nära samverkan med användaren för att på så sätt få ökad acceptans. Sitic som organisation verkar inte vara förankrad hos myndigheter och företag. Vissa myndigheter som har intervjuats i denna uppsats kände knappt till organisationen.

Sitics rapporteringssystem måste vara utformat på ett sätt som gör att organisationer som rapporterar kan göra det så smidigt som möjligt och samtidigt använda så lite resurser som möjligt. Kommunen i denna undersökning ville exempelvis ha mer riktade säkerhetsråd och Myndigheten önskar ett system där alla i organisationen kunde rapportera direkt en incident uppkommer. (mer om detta i kapitel 5.9).

Johansson och Lundevall nämner i sin rapport att för att få de anställda att rapportera incidenter krävs det att rapporteringen är enkel och snabb att utföra. Detta är ett problem också hos vissa organisationer i min undersökning då det hos dessa organisationer endast är en grupp informationssäkerhetsansvariga som har hand om incidentrapportering.

5.7 Rutiner

Företag och organisationer har alla olika rutiner för incidenthantering i allmänhet och incidentrapportering i synnerhet. Allen nämner (rubrik 2.2.1) att dessa rutiner skulle underlättas med hjälp av ett internt incidentrapporteringssystem.

Det universitet som jag har intervjuat beter sig på lite olika sätt beroende på vilken sorts incident det handlar om. Eftersom alla universitet och högskolor i Sverige använder SUNETs nät sker denna incidentövervakning centralt och till stor del automatiskt av SUNET.

Företaget har en som är ansvarig för informationssäkerheten, men har inga ingående rutiner för rapportering av incidenter. De har ett visst samarbete med säkerhetsföretag, men det sker utan rutiner när incidenter inträffar.

Respondenten hos kommunen tycker att Sitic borde ha ett system som möjliggör att varje enskild organisation kan anmäla vilka applikationer och operativsystem de använder sig av för att Sitic på så sätt skulle kunna varna och ge råd för sådant som individuellt för olika organisationer. Varje organisation skulle då få relevant information och slippa leta bland onödig information.

Myndigheten tycker att det borde finnas ett internt incidentrapporteringssystem hos deras organisation, något som saknas idag. Detta system borde användas av all personal och skulle kunna fungera på så sätt att det finns en ikon på skrivbordet på den anställdes dator där denne kan rapportera incidenter internt. Denna information skulle skickas till säkerhetsansvariga på organisationen. Informationen undersöks och bearbetas och skickas sedan vidare till exempelvis Sitic.

6 Resultat

Uppsatsen vill visa på vilka rutiner organisationer, myndigheter och inte minst Sitic har och bör ha för att rapportera incidenter, ta del av incidentinformation och sprida information.

Det har framkommit att Sitics rutiner i vissa fall är bristfälliga. Exempel på detta är att Sitic enbart är verksamt på kontorstid och att de varningar som Sitic går ut med först gås igenom noggrant och sedan översätts till svenska, vilket gör processen långsam.

Företag och organisationer har alla olika typer av problem och skulle därför behöva incidenthanteringspartners som ser just deras problem och som har kunskap om just deras applikationer, operativsystem, virusskydd med mera. Mycket av den information de får från organisationer av Sitics typ är alltför allmänna och passar inte för dem. Det blir därför mer intressant för organisationer att ta hjälp av säkerhetsföretag som är specialiserade på vissa applikationer.

Flera av respondenterna nämner att ett enkelt rapporteringssystem bör finnas hos varje organisation där användare på ett enkelt och inte alltför resurskrävande sätt kan rapportera direkt när de upptäcker brister. Grundläggande rutiner för rapportering av incidenter finns redan hos organisationerna, men stödet för dessa rutiner skulle kunna förbättras så att rapporteringen skulle bli mer effektiv.

Vissa rutiner skulle kunna förbättras både hos Sitic och hos de ”rapporterande” organisationerna. Det har framkommit att Sitic känns som en stor och därför långsam myndighet som inte är kapabel att snabbt varna för nya hot som uppstår. Detta skulle kunna åtgärdas delvis genom att Sitic inleder jourverksamhet, vilket skulle ge snabbare varningar och större förtroende. Någon respondent nämnde också att Sitic bör rikta sin verksamhet på kundens specifika program och applikationer så att de inte riskerar att överhopas av information.

De slutsatser jag drar av detta arbete är att Sitic på något sätt skulle underlätta för organisationer att på ett mera automatiskt och naturligt sätt genomföra sin rapportering. Exempelvis skulle det kunna vara så att när ett företag skickar en rapport till en valfri incidentorganisation, skulle en kopia automatiskt skickas till Sitic. Denna automatik kan visserligen ses som en tvingande åtgärd. Organisationerna i min undersökning skulle, om jag har uppfattat dem rätt, inte ha någonting emot detta, då det inte är sekretesskäl som ligger bakom den bristfälliga rapporteringen.

Sitic bör också möjliggöra för organisationer att prenumerera på vissa tjänster som gäller en specifik applikation eller program, vilket skulle göra att säkerhetsarbetet blir effektivare och överflödig information skulle kunna undvikas.

7 Metoddiskussion

Jag har genom litteraturstudier och en empirisk undersökning genomfört arbetet som har resulterat i denna uppsats. Mitt val av metod har jag gjort utifrån litteratur som behandlar rapportskrivning.

Validiteten, det vill säga att jag mäter det jag avser att mäta, har kunnat säkerställas tack vare diskuterande intervjuer där jag har fått djupare förståelse för den underliggande synen på de saker jag har frågat om. Det faktum att jag har behövt komplettera intervjuerna i efterhand har ökat validiteten. Validiteten handlar alltså om relevansen av insamlad data, för undersökningens problemställning. I min uppsats bör jag därför ställa mig frågan om jag i empirin har ställt sådana frågor som hjälpt mig att besvara forskningsfrågan. Visserligen har inte alla intervjufrågor ett direkt samband med forskningsfrågan men är ändå viktiga för helhetsbilden.

Reliabiliteten i den här uppsatsen har varit svårare att tillfredsställa eftersom jag bara har genomfört en intervju hos var och en av organisationerna som ingår i undersökningen. Det är möjligt att en annan person i den organisation jag har undersökt hade svarat annorlunda på frågorna, Svaren som jag har fått under intervjuerna bör inte ses som den allmänna inställningen hos organisationen i stort. Eftersom jag har för avsikt att intervjua personer med liknande ställning (IT-ansvariga) i alla organisationer, anser jag ändå att intervjuerna ger en acceptabel bild av verkligheten.

Att undersöka de rutiner som organisationer använder sig av vid rapportering av incidenter kan vara svårt, eftersom det är ett känsligt område och någonting som organisationerna inte gärna vill prata med andra om. Trots att jag försäkrar dem om anonymitet kan det vara besvärande för respondenterna att ”avslöja” känsliga arbetssätt för incidenthantering, som om dessa blir kända kan vara till skada för organisationen. Detta gör att jag riskerar att gå miste om viktig information som skulle kunna vara till nytta för rapportens trovärdighet.

8 Diskussion

Jag har under arbetets gång sett att incidentrapportering är ett komplext område och att orsakerna till de låga rapporteringstalen kan vara av många olika slag.

Företag och organisationer har visserligen något bristfälliga rutiner för rapportering, men det största problemet ligger i att organisationerna har svårt att se nyttan av att rapportera till Sitic. Detta beror på att många organisationer redan idag har tillfredsställande samarbeten inom säkerhetsområdet med externa aktörer. Sitic har med andra ord varit för sent ute och inte kunnat förklara nyttan av en nationell incidenthanteringsorganisation.

Det har även framkommit att Sitic riktat sin marknadsföring endast till ett fåtal organisationer. Att man efter två år inte har hunnit arbeta med utåtriktad verksamhet kan tyda på problem med exempelvis finansiering av verksamheten.

En annan orsak till det bristande intresset kan vara att själva företeelsen inte är förankrad i de olika organisationerna som ska samarbeta med Sitic. Det verkar som om de tänkta användarna inte har varit med från start i utvecklingen av Sitic och därför inte kunnat utforma denna verksamhet som de vill.

Problemet för Sitic har enligt dem själva i inledningsskedet varit sekretesslagstiftningen som gjort att de inte har kunnat försäkra inrapportörerna om anonymitet. Detta har gjort att förtroendet för Sitic från början var lågt. För att få förtroende måste en stabil organisation skapas där lagar, regler och rutiner är noga bearbetade.

De flesta organisationer har i dagsläget teknisk möjlighet att rapportera incidenter och gör det också vid vissa incidenter. Samtliga av de organisationerna jag har varit i kontakt med har idag samarbete med olika organisationer (CERT, SUNET-CERT, säkerhetsföretag med flera) vilket gör att många i dagsläget inte känner något behov av att rapportera till Sitic.

Det stora problemet verkar inte ligga i tid och pengar hos företagen (trots att någon nämnde det). Organisationerna skickar redan idag rapporter och tar del av incidentinformation av andra säkerhetsföretag. Att det trots allt inte fungerar på ett tillfredsställande sätt tror jag beror på att organisationer helt enkelt inte känner till möjligheten eller att de inte ser några omedelbara fördelar för den egna organisationen.

9 Referenser och litteraturförteckning

[ALL01] Allen, J. H, 2001 “CERT Guide to System and Network Security Practices”
Addison Wesley ISBN 0-201-73723-X

[AWA04] Awad, E. och Ghaziri, H. (2004) ”Knowledge management”
Pearson Education, New Jersey, ISBN 0-13-034820-1

[CER05] www.cert.org/faq/cert_faq.html#A2 (04-12-10)

[CHR03] Christiernin, A. och Eriksson, B. (2003) ”IT-incidenthantering inom sjukvården i Stockholm läns landsting”
Institutionen för data- och systemvetenskap
Stockholms universitet/Kungliga Tekniska Högskolan

[HÅK03] Håkansson, M. & Wedefelt, F. (2003) ”Kunskapsdelning i nätverksföretag”
Institutionen för informatik
Handelshögskolan vid Göteborgs universitet

[IDG05] www.idg.se/ArticlePages/200401/30/20040130170600_IDG.se027/2004 0130170600_IDG.se027.dbp.asp (2005-01-14)

[ITK05] http://www.itkommissionen.se/dynamaster/filearchive/020124/1d770221ea142a7f79d9137f07089b9e/Remissvar%20Incidenthantering.pdf (2005-06-16)

[JOH00] Johnsson, G. och Wojciechowska, D. (2000) “Rapporteringssystem för incidenter och olyckor”
Institutionen för kemiteknik
Kungliga Tekniska Högskolan

[JOH02] Johansson, M. och Lundevall, P. (2002) ”Design av system för inrapportering
av IT-säkerhetsincidenter”
Institutionen för Data- och Systemvetenskap, DSV
Stockholms Universitet

[MAN01] Mandia, K. och Prosise, C. (2001) ”Incident Response”
Osborne McGraw Hill, ISBN 0-07-213182-9

[MIT02] Mitrovic, P. (2002) ”Handbok i IT-säkerhet”
Pagina Förlags AB, Göteborg, ISBN 91-636-0750-6

[NYT05] http://www.nyteknik.se/pub/ipsart.asp?art_id=27305 (2004-12-10)

[OSC01] Oscarson, P. (2001) ”Informationssäkerhet i verksamheter” Licentiatexamen Linköpings universitet, ISBN 91-7373-242-7

[PAT03] Patel, R. och Davidson, B. (2003) ”Forskningsmetodikens grunder” Studentlitteratur, Lund, ISBN 91-44-02288-3

[SIT05] www.sitic.se (2004-12-01)

[STA05] http://www.sitic.se/dokument/Statskontoret_och_IT-kommissionen-Hantering_av_IT-incidenter.pdf (2004-11-30)

[WOR05] http://lnweb18.worldbank.org/oed/oeddoclib.nsf/interpgname/ksprecis/$file/precis234.pdf (2004-11-25)

[ÖCB05] http://www.sitic.se/dokument/Overstyrelsen_for_Civil_Beredskap-IT-incidenthantering.pdf (2004-12-10)

Bilaga 1. Frågemall

- Vad är din uppgift/position i organisationen?
- Brukar ni rapportera och ta del av incidentinformation till/från någon organisation?
- Känner ni till Sitic?
- Skulle ni kunna tänka er att rapportera?
- Ser ni några *fördelar* med ett nationellt IT-incidenthanteringscentra?
- Ser ni några *nackdelar* med ett nationellt IT-incidenthanteringscentra?
- Har ni blivit hjälpta av Sitic eller någon annan organisation?
- Har ni tekniskt sett möjlighet att rapportera?
- Ser ni några hinder med att dela med er av incidentinformation?
- Känner ni till att en lagändring genomförts angående offentlighetsprincipen och har det gjort att ni hellre rapporterar?
- Saknar ni något hos incidenthanteringsorganisationerna?
- Hur ser ni på en eventuell skyldighet att rapportera?
- Hur ska ett bra system för extern incidentrapportering vara utformat?
- Vad har ni för rutiner vad gäller rapportering av IT-incidenter, internt och externt?
- Har ni något internt incidentrapporteringssystem i vilket användare i organisationen kan rapportera själva?
- Har ni någon ansvarig IT-säkerhetsgrupp i organisationen?