Vilken hotbild har olika branscher vid användning av Internet och hur nyttjas skyddsåtgärderna.

(HS-IKI-EA-04-601)

Rakhi Parmar (a99rakpa@ida.his.se)

Institutionen för datavetenskap
Högskolan i Skövde, Box 408
S-54128 Skövde, SWEDEN

Examensarbete inom informationssystemutveckling under höstterminen 2003

Handledare: Lennart Börjesson

Vilken hotbild har verksamheter vid användning av Internet och hur nyttjas skyddsåtgärderna.

Examensrapport inlämnad av Rakhi Parmar till Högskolan i Skövde, för kandidatexamen (b.Sc. vid Institutionen för Datavetenskap.

[ ]

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._____

Vilken hotbild har olika branscher vid användning av Internet och hur nyttjas skyddsåtgärderna?

Sammanfattning

Avsikten med detta examensarbete var att belysa de faktorer som har betydelse för god IT-säkerhet i ett svenskt företag.

I examensarbetet utreds de hot som finns mot företags IT-system vid en anslutning till Internet, samt vilka skyddsåtgärder som bör nyttjas för att skydda sig mot dessa hot. Rapporten leder fram till vilka hot och skyddsåtgärder som är aktuella för svenska företag. Examensarbetets frågeställning skall innefatta en undersökning av vad verksamheter från två olika branscher tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretagföretag har för hotbild vid en anslutning till Internet samt hur vanligt det är med de olika skyddsåtgärderna. De hotbilder och skyddsåtgärder som valts att använda i arbetet har tagits fram ur en litteraturstudie. Informationssäkerhet skapar huvudsystemet IT-säkerhet som används för skyddsåtgärder som är av teknisk karaktär, t.ex. olika former av behörighetskontrollsystem.

Arbetets problem har gått ut på att få en inblick i hotbilden samt skyddsåtgärder vid en anslutning till Internet bland olika verksamheter tillhörande tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag. Undersökningen baseras på intervjuer kombinerat med litteraturstudier. Verksamheterna som har studerats verkar inom olika verksamhetsområden och branscher.

Undersökningen har påvisat att hotbilden enligt litteraturstudien är ett absolut hot mot verksamheterna även om de inte drabbat alla samt att nämnda skyddsåtgärder enligt litteraturstudien anses vara mycket nödvändiga. Dock skiljer sig hotbilden samt prioritering av skyddsåtgärder mellan tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag. Att hotbilden skiljer sig åt beror på att vissa branscher är mer drabbade än andra.

Nyckelord: IT-säkerhet, Hotbild, Skyddsåtgärder, Internet

Innehållsförteckning

1 Introduktion

IT- säkerhet är ett ämne som fått allt större uppmärksamhet i media för varje dag som gått de senaste åren. Det är i stor utsträckning Internets genomslag som ligger till bakom detta enorma intresse. Internet har fört med sig nya och större risker för angrepp mot våra IT-system som delvis förändrar metoderna i IT-säkerhetsarbetet (IFI, 2003).

Borg m.fl. (1997) hävdar att experter räknar med att antalet attacker mot IT-system anslutna till Internet fördubblas varje år. Med tanke på företags och organisationers beroende av datorer för bokföring, lagring av information och databehandling är detta en oroväckande utveckling. Ju mer beroende verksamheten är av det IT-system, desto större konsekvenser medför en attack eller annan typ av avbrott (Borg m.fl., 1997). Utnyttjandet av Internet samt den ökande elektroniska handeln gör att risken ökar för att personer ska lyckas få tillgång till information de inte har rätt till (SOU, 2001).

Hur väl företag, myndigheter och olika länder i Europa och övriga världen väljer att satsa på IT-säkerhet varierar stort. Arbetet för IT-säkerhet måste breddas och lyftas över den nationella nivån menar EU- kommissionen (Dagens Nyheter, 2003).

Eftersom företagen är beroende av information, ökar även vikten av informationstillgångarna och behovet att skydda dem. Den utrustning som krävs för att skydda information vid överföring och användning utav information innefattas under begreppet IT-säkerhet. Den kontinuerliga utvecklingen inom IT-området gör att förutsättningarna för IT-säkerhet ständigt förändras och därmed bör även skyddsmekanismerna ständigt utvecklas för att det inte skall uppstå brister. Det är inte bara den tekniska utvecklingen som är det viktiga i säkerhetsarbetet, utan krav som ställs på IT-säkerheten i en organisation såsom relation mellan arbetsgivare och personal som hanterar information börjar också få en allt mer framträdande roll (Borg m.fl., 1997).

1.1 Syfte, målgrupp

Syftet med denna uppsats är att ur ett företagsperspektiv belysa de faktorer som svenska företag uppfyller som är av betydelse för god IT-säkerhet i svenska företag. För att åstadkomma detta skall anledningen till det uppfattade av IT-säkerhet undersökas, d.v.s. vilka de vanligaste hoten är som förekommer mot IT-system vid anslutning till Internet . När hotbilden kartlagts ställs frågan hur IT-system skall skyddas mot dessa hot, d.v.s. vilka skydd och lösningar som finns att tillgå.

Uppsatsen riktar sig emot svenska företag och andra intresserade av säkerhetsfrågor ur ett företagsperspektiv.

2 Bakgrund

Detta kapitel avser att förklara och utveckla några av de centrala begrepp som kommer att användas i denna rapport och som är av intresse för rapportens mål och syfte. Detta kapitel blir även en sammanfattning av en del av den kunskap som finns kring rapportens huvudämne och problemställning som redovisas i kapitel 3.

2.1 Informationsteknik (IT)

Med informationsteknik (IT) menas den teknik som används för insamling, lagring, bearbetning och överföring av information med elektroniska medel. Begreppet IT sammanfattar alla de informationshanterande processer inom en organisation som automatiserats och effektiviserats med hjälp av ny teknik; moderna telefonsystem, voicemail, fax, men framför allt datorer och de system som byggts kring och med hjälp av dess komponenter (Borg m.fl., 1997).

IT har i många sammanhang blivit ett bekvämt hjälpmedel som var svårt att föreställa sig för bara något decennium sedan. De positiva effekterna av IT berör de allra flesta i samhället allt från privatpersoner till näringsliv och offentlig verksamhet. Denna utveckling av att IT berört fler och fler personer positivt har bidragit till att samhället har blivit starkt beroende av IT. IT har blivit den viktigaste hjälpmedlet för informationsförsörjning, oavsett om det gäller information till privatpersoner, företagsinformation eller någon annan typ av information. Information är en av de värdefullaste tillgångarna i dagens samhälle enligt (SOU, 2001). IT är ett globalt område och man kan med hjälp av Internet ha kontakt med organisationer och personer på andra sidan jordklotet. Med den gränslöshet som IT-området präglas av följer också ett starkare behov av IT-säkerhet och krishantering (SOU, 2001).

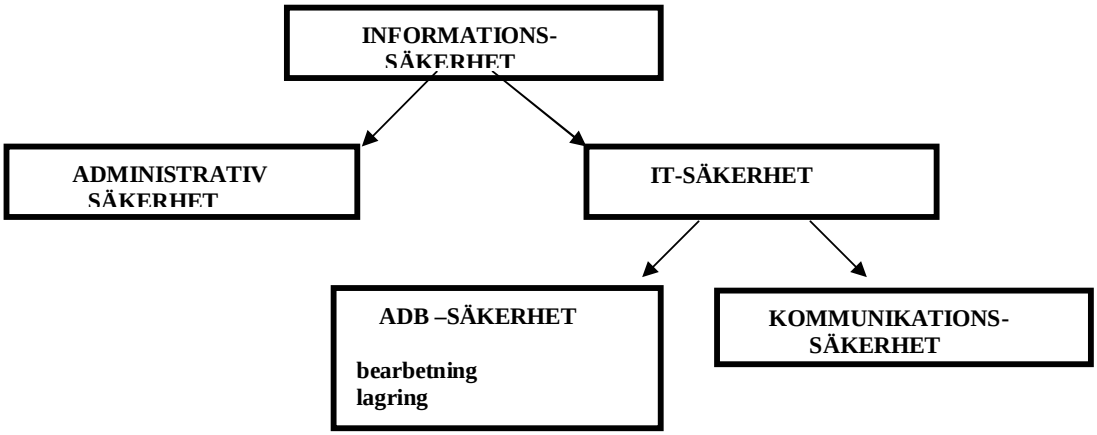
2.2 IT-säkerhet, strukturell uppbyggnad

För att säkra informationen, så att t ex obehöriga inte manipulerar den, krävs en helhetssyn på **informationssäkerheten.** Det är inte bara hemlig, känslig eller värdefull information som måste skyddas. Öppen information är oftast lika känslig vad gäller t.ex. obehörig förändring, vilket kan göra att informationen blir felaktig. För att nå upp till önskad skyddsnivå så behövs det i många fall en kombination av olika skyddsåtgärder.
Tekniska säkerhetslösningar räcker oftast inte till utan det behövs även olika administrativa rutiner såsom katastrofplanering, plan för utbildning av användare m.m.(Statskontoret, 1998a)

Med anledning av ovanstående Informationssäkerhet skapas därav två huvudsystem. Det handlar i ena fallet om **IT-säkerhet** som används för skyddsåtgärder som är av teknisk karaktär, t.ex. olika former av behörighetskontrollsystem. IT-säkerhet inkluderar både ***ADB-säkerhet*** och ***kommunikationssäkerhet***. Med ADB-säkerhet/datasäkerhet menas säkerhet som rör själva behandlingen och/eller lagringen av data (program och information). Kommunikationssäkerhet avser säkerhet vid överföring av data via något kommunikationsmedium. I andra fallet handlar det om den **administrativa säkerhet** som

främst innebär definition av regler och rutiner för styrning och kontroll av IT-resurserna. De tekniska skyddsåtgärderna måste i många fall kompletteras med administrativ säkerhet i olika former. Administrativ säkerhet kan fungera som ett komplement till en teknisk skyddsåtgärd men kan också fungera som en skyddsåtgärd i sig. (Statskontoret, 1998a).

I båda fallen handlar det om att skydda den aktuella informationen både när den hanteras på olika sätt och när den endast passivt lagras för kommande användning.



Figur1: Informationssäkerhetens omfattning (efter Statskontoret, 1998a, s.7).

2.3 Vilka grundkrav ställs på IT-säkerheten?

I takt med att användningen ökar även kraven på IT-systemen. Krav på IT-säkerheten kommer från olika intressenter såsom leverantörer, kunder, myndigheter, banker m.fl.. I detta kapitel behandlas de grundläggande aspekterna kring. IT-säkerhet. Syftet är att på ett tydligt sätt kunna strukturera de olika kraven på IT-säkerhet i fyra tillstånd (Statskontoret, 1998a).

2.3.1 Riktighet

Vad som menas med riktighet är att användardata eller andra IT-resurser som tillhandahålls, t.ex. program och nät, ska ha den rätta kvaliteten. Enligt Statskontoret (1998) och SIG security (1998) kan man säga att den information som systemet tillhandahåller ska vara objektivt sett felfri, vara noggrann, ha rätt detaljeringsgrad, vara aktuell, vara fullständig, vara tillförlitlig och vara konsistent. Det är dessutom viktigt att viktig information är förhindrade av otillåten modifiering av information och resurser vid ändring, duplicering, förfalskning etc. Riktighet är ett samlingsbegrepp för begreppen personintegritet, systemintegritet och kvalitet. Men integritet menas att helheten ska skyddas mot obehörig förändring. Om riktigheten inte fullföljs leder detta till en förlust av integriteten i användardata eller andra IT-resurser som tillhandahåller servrar, program och nät. Förlusten kan orsakas av avsiktliga eller oavsiktliga obehörig förändring av data, tillägg eller radering av meddelande eller data i databaser, filer, kommunikationstrafik, o.s.v. (Statskontoret, 1998c).

Dålig kvalitet på informationen kan exempelvis leda till att:

- Felaktig information sprids internt och externt.
- Beslut fattas utifrån felaktiga underlag
- Personalen drabbas av extra arbete.
- Företag kan förlora kunder och myndigheter kan bli föremål för negativ publicitet i massmedier.

2.3.2 Tillgänglighet

Enligt Statskontoret (1998c) och SIG security (1998) innebär Tillgänglighet (availability) att möjligheten finns för behöriga användare eller andra resurser att utnyttja definierade resurser efter behov, i förväntad utsträckning och inom önskad tid. När tillgängligheten inte är tillräcklig hindras behöriga användare från att utföra sina uppgifter. Exempel på typiska anledningar till tillgänglighetsförlust kan vara driftavbrott och störningar av olika slag.(Statskontoret, 1998c)

Kraven på att systemen ska ha en hög tillgänglighet ökas i samband med att allt mer verksamhet förs över till IT. Eftersom de flesta anställda arbetar direkt med ett eller flera IT-system är det därför viktigt att IT-stödet ska fungera utan störningar. Verksamheter och områden som t.ex. polis, bevakningsföretag, vissa industrier m.fl. kan ha extra höga krav på tillgängligheten där man är beroende av IT-stöd dygnet runt(Statskontoret, 1998b)

Dålig tillgänglighet kan exempelvis medföra att:

- ett visst arbete inte kan utföras i tid
- underlag för beslut kan försenas
- svar inte kan lämnas till externa intressenter som förväntar sig viss service, vilket gör att personalen tvingas ta emot klagomål.
- omvärlden känner misstro mot myndighetens/företagets förmåga att sköta sin verksamhet.

2.3.3 Sekretess

Med sekretess menas att känslig information inte får avslöjas för obehöriga. Förlust av sekretess uppstår när en behörig användare eller en obehörig användare försöker få åtkomst till information som användaren inte har eller ska ha rättigheter till (Statskontoret, 1998c). Ahuja (1996) skriver att hemlig data behöver vara skyddad vid lagring eller vid överföring av data över nätverk. Vid lagring av data kan det vara bra att använda sig utav exempelvis kryptering eller behörighetskontroll. Kryptering bör användas vid överföring av data (Ahuja, 1996).

Sekretess (confidentiality) är enligt SIG security (1998) att hålla information och resurser otillgängliga för obehöriga. Behovet av att skydda information och program till att göra den otillgänglig för obehöriga under lagring, bearbetning och kommunikation finns hos såväl myndigheter som företag. För myndigheternas del ställer sekretesslagstiftningen krav på att viss information skyddas. Datalagen kräver exempelvis att myndigheter såväl som företag skyddar personuppgifter.

I samband med sekretess brukar begreppet konfidentialitet ofta användas.
Konfidentialitet syftar till att skydda hemlig eller känslig information från obehörig insyn (Statskontoret, 1998c).

Om information och program inte skyddas kan det medföra att:

- enskilda personers integritet skadas
- företagshemligheter sprids till obehöriga
- uppgifter som berör rikets säkerhet kommer i orätta händer
- systemet upphör på grund av att någon oavsiktligt eller avsiktligt förstört data eller program
- någon drar åt sig pengar genom otillåten användning av systemet.

2.3.4 Spårbarhet

Spårbarhet och oavvislighet avser skydd och återställande från förlust och brott mot säkerheten. Kravet på spårbarhet är att kunna få användare att hållas ansvariga för sina handlingar i IT-systemet, t.ex. förändringar av systeminställningar, mottagande eller sändande av en informationsmängd eller editiering i olika dokument. Brist på spårbarhet innebär att användarna inte hålls ansvariga för sina förhavanden i IT-området. Systemadministratörer och systemoperatörer kan inte hållas ansvariga för sina administrativa aktiviteter, användarna kan inte hållas ansvariga för sin användning av tjänster eller utförande av transaktioner (Statskontoret, 1998c).

Oavvislighet innebär att en användare i efterhand inte kan förneka att hon/han har skickat eller mottagit ett meddelande. Användaren kan heller inte förneka att hon/han har deltagit i eller orsakat en handling.

Dålig spårbarhet kan innebära att:
- obehöriga aktiviteter inte kan spåras
- upphovsmannen till en transaktion, förnekar exempelvis att han/hon utfört en överföring av en stor summa pengar.

2.4 Definition av hot – risk - sårbarhet

Ett hot är en möjlig oönskad händelse som, om den inträffade, skulle få negativa följder. Det är viktigt att skilja mellan begreppen hot och risk som kan definieras som sannolikheten för att hotet ska realiseras, d.v.s. att händelsen ska inträffa.

Det är viktigt samt nödvändigt att varje organisation känner till vilka hot som finns mot sitt egna system, vilka svagheter systemet har och hur sårbart ett system är för att kunna införa effektiv IT-säkerhet, antingen för en enskild IT-resurs eller för hela organisationen. Denna kunskap är nödvändig för att kunna välja de mest relevanta och kostnadseffektiva säkerhetsåtgärderna (Statskontoret, 1998b).

- Ett **hot** är en handling eller händelse som kan komma att skada en IT-resurs, t.ex. information eller en applikation.

- **Sårbarhet** är en punkt där ett hot kan skada systemet. Sårbarhet är således en svaghet som ett hot kan utnyttja för att åstadkomma skada.

- **Risk** är sannolikheten för att hotet ska realiseras.

Det som är nytt i informationsåldern är dels att informationen är mindre fysiskt påtaglig och att ofantligt mycket mer information kan lagras på samma utrymme. Hoten blir dels allt otydligare samt att angriparen inte behöver befinna sig på samma plats som informationen lagras. Angriparen behöver inte ens befinna sig i samma land som information lagras (SIG Security, 1998).
Hot kan enligt (Statskontoret, 1998c) delas upp i tre kategorier:

- ***Logiska hot*** är hot mot IT-resurser, funktioner och tjänster. Dessa förhindras av logiska skyddsåtgärder

- ***Administrativa hot*** är hot mot administrativa rutiner och organisatoriska lösningar. Dessa förhindras av administrativa skyddsåtgärder.

- ***Fysiska hot*** är hot av typen skadegörelse, miljöpåverkan eller stöld. Dessa förhindras av byggnadstekniska skyddsåtgärder.

2.4.1 Oavsiktliga och avsiktliga hot internt/externt

Brister i administrativa rutiner och i själva IT-verksamheten är exempel på mycket vardagliga händelser som är de vanligaste hoten mot IT-verksamheten. Interna hot tillhör för det mesta kategorin som brukar kallas ***oavsiktliga*** hot. Organisationer som utnyttjar informationsteknik i någon form drabbas mer eller mindre av oönskade händelser t.ex. genom överföringsfel. Utöver de oavsiktliga hoten förekommer även de ***interna avsiktliga*** hoten.

Organisationer kan även utsättas för externa hot, som är vad man oftast betecknar som ***avsiktliga*** hot, d.v.s. att någon obehörig enskild eller en organisation exempelvis försöker komma åt viss information eller försöker sabotera hela IT-verksamheter. Det är viktigt att man måste ha klart för sig vilka interna och externa, avsiktliga respektive oavsiktliga hot som är relevanta i den egna verksamheten, samt vara medveten om att kunna bedöma hur stor sannolikheten är att hoten skall utlösas. Enligt Statskontoret (1998c) är de oavsiktliga hoten erfarenhetsmässigt relativt många i IT-verksamheter.

2.4.2 Definition av Internet och World Wide Web

Internet betyder mellan nätverk. Internet är en sammankoppling av datorer över hela världen. Med datorutrustning, Internetabonnemang och Internetprogram kan människor söka och även hämta hem och spara på sin egna dator (Fors, 2003)

Internet är världens största datornät som spänner över alla kontinenter samt en enorm källa till information om allt mellan himmel och jord. Internet är drygt 32 år gammalt. Det är dock på senare tid (ca 17 år) som nätverket fått en riktig stor internationell spridning. Svenska försvaret var en av dem som var med och startade utvecklingen av Internet i Sverige. Utgångspunkten var att forskare, utvecklare och militärer inom alla de universitet, företag och myndigheter som bedrev forskning och utveckling för det Svenska försvaret skulle kunna kommunicera med varandra över ett datornät. Man skulle kunna skicka elektroniska brev till varandra, föra över data mellan olika datorer och kunna köra program på datorer över hela landet från sin egen terminal (Andersson, Carlsson & Åkerman, 1996).

I Sverige finns det flera sätt att komma in på Internet. Från början var det dock endast institutioner inom högskolevärlden som via det svenska universitetsnätet (SUNET) kunde komma ut på Internet. Det första kommersiella företag som erbjöd Internet i Sverige var

Tele2 med sitt Swipnet. Telia (dåvarande Televerket) följde efter med sitt TIPNET. Sedan dess har ytterligare nätoperatörer tillkommit (Andersson, Carlsson & Åkerman, 1996).

World Wide Web (WWW) är Internets multimediatjänst och ett sätt att kommunicera. WWW består av sett stort antal sidor som finns lagrade på datorer runt om i världen, här kan man se bilder, läsa texter, höra ljud och se rörliga bilder. WWW är lätt att använda och uppbyggnaden gör det mycket lätt att snabbt söka sig fram till det man letar efter (Andersson, Carlsson & Åkerman, 1996).

2.4.2.1 Anslutning till Internet

Internet kan dels användas genom en uppringd förbindelse som är ett vanligt förfarande för enskilda arbetsplatser, och dels fast anslutning där en router förbinder ett lokalt nät med Internet. Fast anslutning används vanligtvis när flera arbetsplatser ska ha tillgång till Internet. De hot och risker som är aktuella vid anslutning till Internet gäller i första hand när den egna utrustningen är uppkopplad med fast förbindelse till router eller motsvarande på Internet (Statskontoret, 1998c).

Borg m.fl. (1997) beskriver en fast anslutning som en metod där företagets nät, eller de delar av det som gjorts tillgängliga, alltid åtkomliga för omvärlden. Detta är en metod som gynnar organisationer som vill använda sig av Internet i större utsträckning eller vill erbjuda varor eller tjänster via Internet. Genom uppkoppling mot Internet finns möjligheter till omvärlden att komma åt nätverket genom tänkbara angreppsvägar.

Frågor som organisationen bör ställa sig innan man kopplar upp enligt Borg m.fl. (1997) är:

Vilka är riskerna? När en organisation väljer att koppla upp sig mot Internet ger man en målmedveten angripare en till möjlig ingång till systemet, men viktigare: Man öppnar upp en möjlig ingång för folk som kommer att försöka angripa nätverket bara för att det går.

Vilka konsekvenser får ett intrång utifrån? Vad händer om information stjäls eller förstörs som konsekvens av ett intrång? Vad händer om systemet inte är tillgängligt under en tid till följd av ett intrång.

Vilka punkter i systemet löper störst risk att attackeras utifrån? Hur ska man se till att hålla en jämn säkerhetsnivå, så att inte massor av tid och resurser läggs på att säkra vissa delar av systemet medan andra punkter är helt oskyddade.

Dessa punkter är naturligtvis bara en delmängd av den säkerhetspolicy som organisationen bör ha eller utarbeta.

2.4.2.2 Externa och logiska hot som förekommer vid anslutning till Internet

Det är viktigt att organisationer inser att de ***externa hoten*** mot IT-systemet också är en realitet. Exempel på hot och risker vid obehörigt intrång enligt Statskontoret (1998b) är:

- En ”***hacker***” kommer åt information genom att ta sig in i ett stordatorsystem.

- ***Inloggning under falsk identitet*** uppstår när obehöriga användare eller ett obehörigt program loggar in under falsk identitet.

- ***Obehörig åtkomst*** uppstår när en extern eller en intern behörig användare lyckas gå förbi reglerna för åtkomstkontroll, t.ex. genom att åtkomstkontrollistan modifieras.

- ***Avlyssning eller informationsläckage*** uppstår när obehöriga användare avlyssnar kommunikationen mellan två parter. När en annan användare än avsedd mottagare avsiktligt eller oavsiktligt får tillgång till ett meddelande eller andra informationsmängder handlar detta om att obehörig insyn uppstår.

- ***Modifiering/tillägg/borttagning av information*** uppstår när det sker en avsiktlig eller oavsiktlig modifiering, tillägg eller radering av meddelanden, data eller program i databaser eller vid överföring. Detta kan även gälla ändring av textinnehåll på webbsidor.

- ***Modifiering/tillägg/borttag av program*** uppstår oftast genom olika ***datavirus*** som ingår i någon form av illasinnad funktion och nätet drabbas av virus via disketter, överförda filer som bifogats via e-post eller tagit hem via Internet.

2.4.2.3 Definition av virus

Ett av de mest tydliga generella hoten är virus. Virus är ett program som mångfaldigar sig utan användarens tillstånd. Virusets syfte är att få så stor spridning som möjligt. Ett datavirus kan jämföras med ett biologiskt virus som använder celler som värdkroppar för att producera nya exemplar av viruset. Ett datavirus är beroende av andra program eller filer för att överleva och spridas måste det under en viss period vara inaktiv. Ett datavirus består huvudsak av två delar, en kopierande del och en förstörande del (Nordstedts ordbok AB, 1999).

Ett virus introduceras i system i samband med installation eller överföring utav ”smittad” programvara och har som effekt att vid en exekvering kunna överföra en, möjligt förändrad, kopia av viruset till andra program (Nordstedts ordbok AB, 1999).

2.4.2.4 Definition av hacker

En hacker är i sin ursprungliga form en uppskattande hederstitel som användes för att beteckna en person som på ett exceptionellt sätt behärskade den nya tekniken. En hacker var en person som gjorde bra och snygga ”hack”, där hack betecknar en ofta originell och kanske oväntad lösning på ett problem. Vid slutet på sjuttiotalet och början på åttiotalet började den nya tekniken bli allt synligare som fick media att uppmärksamma hackerkulturen. I media blev hacker under åttiotalet synonymt med de som utnyttjade sin kunskap för att ta sig in i datorsystem (Borg m.fl., 1997). Ordet "hacker" fick under mitten av 80-talet en negativ laddning, eftersom många datorfantaster ägnade sig åt att bryta sig in

i olika datorsystem. Från att ha varit en entusiastisk datorfantast, blev han nu en farlig datorfantast.

Syftet med hackerns intrång kan naturligtvis variera. Några tar sig bara in för att se om det går eller för att se vilka filer som finns. Andra är ute efter att sabotera den data som finns lagrad, t.ex. ändra innehållet i ett dokument eller förstöra filer genom att radera dem. Sedan finns det några som försöker utnyttja datorn för att sprida virus eller maskar. Ordet "hacker" kan i vissa sammanhang även få en positiv laddning.

När man fått skrivaren att fungera på kontoret, trots att inte ens teknikerna klarade det, säger man stolt att man "hackat systemet". En hacker är då en person som klarar av det till synes omöjliga, att förbättra prestandan på en hård- eller mjukvara. I denna innebörd finns ibland också synsättet att hackern gör dessa förbättringar på ett okonventionellt sätt, alltså ett sätt som inte handboken eller manualerna beskriver. Hackern blir då lite hemlig. Men när det okonventionella övergår i att vara olagligt, brukar de flesta vända i sitt synsätt och se hackern som potentiellt farlig. På så vis kan den positiva laddningen lätt slå över i en negativ (Nordstedts ordbok AB, 1999). Begreppet "hacker" är ganska brett och tack vare sin historia också ganska svårbestämt. Ordet kan användas om flera olika företeelser och ha både bra och dålig laddning.

2.5 Skyddsåtgärder

För att uppnå informationssäkerhet, det vill säga skydda sin information, så måste man använda olika skyddsåtgärder. Skyddsåtgärder används för att möta speciella hot. Vissa skyddsåtgärder kan möta fler än ett hot. Vissa hot bekämpas mer effektivt genom att flera olika skyddsåtgärder samverkar (Statskontoret, 1998a) . För att uppnå högsta möjliga skyddsnivå så måste skyddsåtgärder av de tre typerna kombineras på ett lämpligt sätt, det vill säga anpassas till verksamhetens typ (Statskontoret, 1998c).

Skyddsåtgärder kan delas in i tre kategorier:
• ***Logiska skyddsåtgärder,*** är skyddsåtgärder av teknisk karaktär i form av maskin- och/eller programvara.
• ***Administrativa skyddsåtgärder****,* är regler och rutiner för vilka arbetsmoment som måste genomföras och hur.
• ***Byggnadstekniska skyddsåtgärder****,* är skyddsåtgärder av fysisk karaktär som till exempel lås.

Skyddsåtgärder kan användas på olika sätt, till exempel för att förebygga, upptäcka och varna för hot eller för att återställa det som skadan ställde till med. Att *förebygga* ett hot är det bästa alternativet. Det innebär att hotet inte kan utnyttja en sårbarhet. I vissa lägen är det inte möjligt att förebygga ett hot. Skyddsåtgärden kan då *rapportera* skadan. Det finns också skyddsåtgärder som kan *återställa* eller *begränsa* följderna av hotet efter det har inträffat.

Nedan presenteras några av de vanliga ***logiska skyddsåtgärder*** som används för att säkerställa IT-systemet.

2.5.1 Kryptering skydd mot överföring av information

För att åstadkomma säkerhet på Internet inom alla elektroniska kommunikationsnät är krypteringstekniken en av de riktigt säkra metoderna. Krypteringstekniken har funnits sedan länge men det är inte förrän under det senaste århundradet som det blivit allt viktigare och behovet ökat hos privatpersoner, företag och organisationer. Risken för intrång samt effekterna av intrång kan med hjälp av krypteringstekniken minskas i hög grad. Med krypteringsteknik är det möjligt att åstadkomma ett nät som på ett säkert sätt kan hantera information. Allteftersom utvecklingen och ny forskning pågår ökar ställs det även större krav på krypteringsalgoritmerna.

Kryptering är en metod som används för att omvandla en läsbar text genom att göra om bokstäver och siffror och flytta runt dem så man döljer dess innehåll. Ett bra exempel kan vara Rövarspråket (Hemligt språk). När en läsbar text krypterats får man en oläsbar ”gibberish” som kallas för chiffertext. Denna chiffertext som man får genom kryptering kan försäkra dig om att information döljs för dem den inte är avsedd för. För att kunna göra chiffertexten läslig igen utförs processen **dekryptering**. Krypteringsteknologin kan även användas för identifikation i nätverkssammanhang, då man vill veta vem man kommunicerar med. Med hjälp av krypteringsteknologin kan man skapa en digital signatur som är en sorts namnteckning eller stämpel på ett dokument. Samma teknologi kan dessutom användas för att kontrollera att dokumentet inte förändrats (Statskontoret, 1998c).

Kryptering används för att :

- Hindra obehörig avlyssning.
- Se till att tjänster och dokument endast är tillgängliga för de som är behöriga.
- Säkerställa att man vet vem som har skickat ett meddelande eller ett dokument.
- Avslöja om ett meddelande har förvanskats.

2.5.1.1 Kryptografiska kontrollsummor

Beräkning av kontrollsummor är en teknik för att kontrollera att det inte förekommit någon manipulation av överförd eller lagrad informationsmängd. Detta anses vara ett bra skydd när någon exempelvis vill försäkra sig om att ekonomiska transaktioner inte utsätts för brott. Beräkning av kontrollsumma är en metod för att beräkna ett unikt värde av en viss informationsmängd. Kontrollsumman kan ses som informationsmängdens ”fingeravtryck”, som sedan används i bl.a. den digitala signaturen (Statskontoret, 1998c).

2.5.1.2 Digital signatur

Digital signatur är motsvarigheten till ”analog” signatur – underskrift med bläckpenna. Den digitala signaturen ska bekräfta innehållets riktighet, vem som ansvarar för dess innehåll. Den digitala signaturen kan ses som ett ”tillägg” till dokumentet och kan kontrolleras av den läsare som vill verifiera innehållet (Statskontoret, 1998c).

2.5.2 Behörighetskontrollsystem (BKS) - Reglera åtkomst

BKS är ett system som kan kontrollera behörighet och som kan skydda information så att den endast är tillgänglig för den som har rätt till den. Ett BKS består utav ett antal samverkande funktioner som tillsammans kan tillhandahåller ett grundläggande behörighetsskydd. Genom att det finns ett behörighetskontrollsystem installerat i datorn som används finns möjligheten att kunna ha kontroll över tillgången till olika resurser i ett IT-system (Statskontoret, 1998c). Mycket av de resurser som leverantörer och användarföretag lägger ned på IT-säkerhetsmekanismer gäller behörighetskontroll, d.v.s. möjligheten att reglera vem som kan använda en systemresurs och på vilket sätt detta kan ske (Lindberg, 1993).

Ett BKS ska kunna:

- Identifiera och *autenicera* behöriga användare

- tilldela och kontrollera *åtkomst*, d.v.s. varje användare ska ha definierad åtkomst till ett antal resurser som han/hon behöver för att kunna utföra sina arbetsuppgifter (resurs är i detta sammanhanget dator, lagringsmedier, skrivare, kommunikationsförbindelser, tillämpningsprogram, hjälpprogram och systemprogram samt alla typer av lagrade data).

- Rapportera alla händelser i såväl BKS som de tillämpningssystem och andra resurser som BKS kontrollerar t.ex. genom *loggar*.

Behörighetskontroll är en funktion som reglerar användarnas och de av användarna startade applikationernas rättigheter på nätverket. Vanligast är att behörighet att läsa, skriva, eller köra filer kan styras individuellt för varje användaren (Borg m.fl., 1997).

2.5.2.1. Identifiering och autenticering

Identifiering innebär att en användare eller en resurs anger sin identitet för att få tillgång till system, information eller liknande. Identiteten kan exempelvis vara ett namn eller nummer. Det är viktigt att identiteten är unik inom ”systemet” så att man kan skilja mellan olika användare. IT-systemets användare ska alltså finnas registrerade i BKS med en egen identitet. Ur säkerhetssynpunkt är det viktigt att motparter kan lita på varandras identiteter (Lindgren, 1993). Eftersom användaridentiteten är öppen information måste den kompletteras med något som varje användare känner till eller har tillgång till, detta för att kunna autenticera/verifiera att en som utger sig för att vara någon verkligen är den personen (Statskontoret 1998c).

För att systemet skall kunna utföra uppgifter åt användaren måste det gå att identifiera användaren, vanligtvis genom ett användarid (Borg m.fl., 1997).

Autenticering innebär kontroll/verifiering av uppgiven identitet, t.ex. vid inloggning, vid kommunikation mellan två system vid utväxling av meddelande mellan användare (Statskontoret, 1998c). En korrekt autenticering av användarna är viktig för effektiviteten hos övriga säkerhetsfunktioner (Borg m.fl., 1997).

Det finns tre tekniker för autenticering av användare eller andra resurser kan identifieras. Dessa tekniker kan användas var och en för sig eller i olika kombinationer:

- Något man *VET* t.ex. ett lösenord, personlig kod/PIN, eller en kombination av fakta från en persons bakgrund (Statskontoret, 1998c). Lösenord är autenticering via något som endast den rätta användaren kan veta (Borg m.fl., 1997).

- Något man *HAR* t.ex. en token, bärare eller krypteringsnyckel (Statskontoret, 1998c). Någonting som endast användaren äger exempel ett smartcard (Borg m.fl., 1997).

- Något man *ÄR* t.ex. biometriska egenskaper som fingeravtryck eller röstmönster (Statskontoret, 1998c). Bygger på något unikt för användaren.

I varje system ska det gå att knyta en viss händelse i systemet till en specifik användare.

2.5.2.1.1 Lösenord

Autenticering kan som nämnts ovan ske på flera olika sätt, vanligast på de flesta datorsystem är lösenord. Det vanligaste sättet att autenticera är att varje användare har ett eget lösenord, som man måste använda tillsammans med användaridentiteten för att få tillgång till ett system eller en delresurs. Lösenorden ska vara unika, svåra och vårdas ömt av den anställde. En bra administratör ser till att det finns en användardatabas o organisationen där alla anställda och deras lösenord finns med (Borg m.fl., 1997).

BKS ska skydda lösenordstabellen mot obehörig åtkomst och det bör också finnas funktioner som gör det möjligt att kryptera lösenordstabellen. För att BKS ska fungera på ett effektivt och ändamålsenligt sätt måste det finnas regler för lösenordshantering (Statskontoret, 1998c).

Det är viktigt att förmedla användarna om hur viktigt hanterandet av lösenordet är för organisationens säkerhet.. Personliga lösenord bör under inga omständigheter lånas ut till tillfälliga användare. Det är även viktigt att användaren inte använder sitt personliga lösenord för organisationens nätverk på organisationsexterna system, som till exempel tjänster på Internet. Det är inte bara tillgången till användarens filer och resurser som äventyras om användaren är slarvig med sitt lösenord, eftersom en inkräktare som genom ett lösenord fått tillgång till systemet, kanske till och med administratörsrättigheter.

2.5.2.2 Åtkomstkontroll

Åtkomstkontroll syftar till att förhindra att en användare får tillgång till andra data, program eller övriga resurser som han eller hon inte behöver till sitt arbete. Hur åtkomstkontrollen skall fungera i en organisation styrs av en mängd faktorer.

Behörighet att få tillgång till olika resurser bör beskrivas i form av behörighetsprofiler, som lagras i BKS. Behörighetsprofilen ska beskriva vilka resurser som ska vara tillgängliga, och ange vad man får göra, t.ex. ta del av information, lägga in nya uppgifter, förändra och ta bort. Varje användare av systemet knyts sedan till den behörighetsprofil som svarar mot de behov användaren har i sitt arbete av att få tillgång till ett visst IT-system eller en viss delresurs (Statskontoret, 1998c).

2.5.2.3 Loggning

Loggning är ett samlingsnamn för de procedurer som sparar ner information om ett systems användande till någon form av permanent lagringsmedia (Borg m.fl., 1997). Ett BKS ska kunna tillhandahålla funktioner så att alla händelser i datorn lagras i en s.k. loggfil. Av loggen ska det bl.a. framgå vilka användare som har varit inloggade i systemet, vilka resurser de utnyttjar och tidpunkten för olika aktiviteter. När olika tillämpningsprogram aktiveras ska loggen innehålla t.ex. uppgift om vem som aktiverat aktuellt program, tidpunkten för detta och även viss information från de bearbetningar som utförts (Statskontoret, 1998c).

I BKS-systemet ska det finnas en särskild logg som registrerar all information om händelser, t.ex. registrering av nya användare och deras rättigheter, ändringar i behörighetsinformation, försök till åtkomst av resurser som man inte är behörig att använda och försöka komma in i systemet med felaktig identitet och/eller lösenord. Logga alltid för mycket än för lite, lyckade som misslyckade försök. Man bör vara medveten om att man sällan vet i förväg vilka händelser som kommer att visa sig vara intressanta när ett angrepp skett. (Borg m.fl., 1997).

2.5.3 Brandvägg

En av de mest använda metoderna för att skydda systemet eller det lokala nätverket från dess koppling med Internet används brandväggar till hög grad. En brandvägg är en av de flera sätt att skydda ett privat nätverk från ett annat nätverk (Vacca , 1996). Statskontoret (1998c) beskriver att en brandvägg består utav en eller flera nätkomponenter som placerats mellan två datornät för att enligt en förutbestämd policy kontrollera och begränsa trafiken mellan dem. De nätkomponenter som ingår i en brandvägg är vanligen routerutrustningar och specialanpassade datorer. Genom brandväggen passerar all trafik mellan de två datornäten, och endast trafik som är godkänd enligt den förutbestämda policyn tillåts passera. Det är även viktigt att brandväggen ska kunna skydda sig själv från angrepp för att kunna erbjuda en så effektiv funktion som möjligt (Statskontoret, 1998c).

Borg m.fl. (1997) menar på att brandvägg är det medel de flesta väljer för att skydda sin organisations nätverk mot otillbörligt intrång från omvärlden. En brandvägg är alltså det

system som skiljer två nätverk från varandra, i det här fallet organisationens nätverk och Internet. Brandväggen är en bra metod att öka säkerheten dramatiskt på sin Internetanslutning. Ett misstag som många gör är att hänga upp hela sin säkerhetspolicy på sin brandvägg. Det är viktigt att inse att en brandvägg skyddar en enskild ingång till organisationens nätverk, och att det skyddet aldrig kan garantera hundraprocentig säkerhet (Borg m.fl., 1997). En brandvägg ska av övervakningsskäl även innehålla funktionalitet för loggning av såväl normal som otillåten trafik och bör erbjuda verktyg för analys av loggad trafik. Vid trafik som indikerar säkerhetsöverträdelser bör det också finnas möjlighet att koppla larm.

2.5.3.1 Vad skyddar en brandvägg mot?

En brandvägg kontrollerar vilka tjänster på det interna nätverket som omvärlden ska få tillgång till. Dessa tjänster är vanligen möjligheten att skicka e-post till eller via en e-postserver på nätverket, eller titta på webbsidor som ligger på en webbserver. Brandväggen kan övervaka hur dessa tjänster används samt att brandväggen kan se till att kontrollera att omvärlden inte kommer åt mer av nätverket än nödvändigt. Med hjälp av en brandvägg kan man kontrollera på vilka sätt det interna nätverket kommer åt Internet. Om en organisation exempelvis har skaffat Internetanslutning enbart för att ge användarna möjlighet att skicka e-post, kan man stänga av alla möjligheter att komma åt Internet förutom just möjligheten att skicka och ta emot e-post.

2.5.4 Antivirusskydd

Skydden man tar till vid virusangrepp ska stå i relation till de skador ett virusangrepp kan förorsaka och en bedömning av hur stor man anser risken för ett angrepp vara.

Vid skydd mot datavirus är det frågan om:

- att förebygga att man överhuvudtaget blir smittad
- att upptäcka ett smittat program och då förhindra smittspridning
- att återställa ett smittat system

Virusprogram bör installeras på flera ställen i IT-miljön. Virusangreppen tacklas då på en bredare och mer heltäckande basis. Virusskydden kan vara av två typer aktiva virusskydd och passiva virusskydd (Statskontoret, 1998c).

Den aktiva programvaran kan startas automatiskt t.ex. vid uppstart av arbetsplatsen. Sedan ligger den minnesresident i bakgrunden och letar kontinuerligt efter virus och virusliknande aktiviteter. Den kan även kontrollera program och datafiler innan de används. Det aktiva skyddet kan även i många fall leta efter misstänkta handlingar vid öppnande och stängandet av fil eller skrivning av fil till lagringsenhet (Statskontoret, 1998c).

Det passiva programvaran kan aktiveras vid specifika tidpunkter t.ex. vid låg belastning för att göra en schemalagd körning.

Yttre anslutningar mot Internet eller andra fjärrnät kan skyddas redan vid brandväggen. Viruskontroll kan här ske på såväl ingående som utgående trafik:

- Kommunikation via elektronisk post och diskussionsgrupper.
- Kommunikation via Webnavigering.
- Filöverföring.

Virusskyddsprogramvaran kan förutom ovan nämnda format stödja även olika paketeringsformat och komprimeringsformat. Virusprogramvaran behövs också en databas med kända virusinstruktioner och signaturer (Statskontoret, 1998c).

3 Problem

Nedan följer en beskrivning av problemområdet och en problemprecisering, därefter görs avgränsningar och det förväntade resultatet presenteras.

3.1 Problemområde

IT-säkerhet är idag ett känsligt och svårbemästrat område. Allt fler företag väljer att ansluta sig till nätverk, vilket betyder att de även utsätter sig för nya hot. Det behöver inte enbart vara hemlig data som behöver skyddas utan även ”vanlig” data. Kraven på att minimera hoten kan komma från många håll, t ex anställda, företagsledning och andra intressenter såsom banker, försäkringsbolag, skattemyndigheter och lagstiftare (Vxu, 2003).

Informationssäkerhet kan delas upp i IT-säkerhet och administrativ säkerhet. IT- säkerhet används för skyddsåtgärder som är av teknisk karaktär, exempel på en teknisk lösning är behörighetskontrollsystem. Administrativ säkerhet uppnås huvudsakligen i form av regler och rutiner för styrning och kontroll av IT-resurserna (Statskontoret, 1998a). För att säkra informationen, så att t.ex. obehöriga inte manipulerar den, krävs en helhetssyn på informationssäkerheten. Det räcker ofta inte med enskilda tekniska säkerhetslösningar utan det behövs även olika administrativa rutiner samt utbildning av användare med mera (Statskontoret, 1998a).

Ett nätverk eller ett system som är kopplat till Internet runt om i världen innebär en stor risk, med tanke på de hackers samt andra obehöriga personer som finns (Vacca, 1996).
Med anslutning till Internet menas den anslutning till det globalt täckande fjärrnät som kallas Internet. De hot och risker som är aktuella vid anslutning till Internet gäller i första hand när den egna utrustningen är uppkopplad med fast förbindelse till router eller motsvarande på Internet. Genom att vara ansluten till Internet bidrar detta till en ökad risk för externa hot samt logiska hot d.v.s. hot mot IT-resurser, funktioner och tjänster. För att åtgärda dessa hot används logiska skyddsåtgärder exempelvis behörighetskontrollsystem m.fl.

Den ökande kommunikationen över Internet, som är känt som ett osäkert media, har dock satt säkerhetsaspekterna i fokus och därmed ökat även medvetandegraden över hoten (Wedberg, artikel 2, 1997). Utnyttjandet av World Wide Web och Internet samt den ökande elektroniska handeln, gör att risken ökar för att externa individer skall lyckas få tillgång till information de inte har rätt till på grund av den ökade exponeringen av den information som hanteras (Kommunikationsdepartementet, 1997). Därmed har också behovet av att skydda sin information från obehöriga ökat.

I takt med användningen ökar även kraven på IT-systemen. Krav på IT-säkerheten kommer från olika intressenter. De fyra kraven på IT-säkerhet är riktighet, tillgänglighet, sekretess och spårbarhet. Genom att använda sig av tekniska skyddsnivåer kan dessa krav uppfyllas i hög grad (Statskontoret, 1998a).

Eftersom litteraturen är väldigt samstämd och ger denna enhetliga hotbild i samband med en anslutning till Internet, är ett grundläggande motiv till denna uppsats att undersöka hur olika verksamheter upplever denna hotbild.

Litteraturen beskriver en generell hotbild som kan drabba samtliga företag och branscher. Detta har väckt funderingar kring om hotbilden verkligen kan ses som generell för samtliga branscher. Det är av denna anledning intressant att undersöka om hotbilden skiljer sig åt mellan olika branscher som tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag. Tjänsteföretag som arbetar mycket med pengar och kan tänkas vara mer utsatta för hot än tillverkandeföretag. Utifrån denna resonerande tanke verkar detta vara ett intressant motiv till denna uppsats.

IT-säkerhet som är så eftersatt på så många svenska företag, är ett annat grundläggande motiv till uppsatsen att undersöka hur nödvändiga olika skyddsåtgärder är för olika verksamheter samt om användning utav skyddsåtgärder påverkas utifrån den hotbild som verksamheterna/branscherna har. Eftersom det finns flera olika skyddsåtgärder som kan användas i samband med en anslutning till Internet, har det valts att endast ta upp de skyddsåtgärder som anses vara vanligast i denna rapport. Syftet med denna undersökning är att ta reda på vilka skyddsåtgärder som används i olika verksamheter och till vilket syfte, samt om verksamheternas hotbild vid en anslutning till Internet påverkar användningen av skyddsåtgärder.

Sammanfattningsvis blir det vetenskapliga bidraget i denna rapport att försöka lyfta fram om den hotbild som tas upp i litteraturen stämmer överens med hur företagen upplever den och samtidigt få fram hur hotbilden skiljer sig åt mellan tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag. Dessutom ska rapporten lyfta fram hur nödvändiga skyddsåtgärderna är för olika verksamheter.

Då säkerheten är så eftersatt på många svenska företag enligt Borg m.fl. (1997), så är det största grundläggande motivet till uppsatsen att studera hur svenska företag som är uppkopplade till Internet upplever den externa hotbild som finns idag samt hur de gör för att erhålla säkra IT-system genom alternativa skyddsåtgärder.

3.2 Problemprecisering

Utifrån problembeskrivningen skall detta examensarbete fokusera på följande problemprecisering:

- Kartlägga om den externa hotbild jag presenterat från litteraturstudier i kapitel 2 stämmer överens med den hotbild verksamheterna upplever vid anslutning till Internet, samt om den skiljer sig åt mellan tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag.

- Undersöka vilka av de nämnda (se kapitel 2.7) säkerhetsåtgärder som används i organisationer vid anslutning till Internet, d.v.s. skydd och lösningar för att åtgärda hoten och till vilket syfte. (Det här för att se om användningen av skyddsåtgärder påverkas utifrån eventuell skillnad av den hotbild verksamheterna har)

3.3 Avgränsning

Eftersom IT-säkerhet är ett så omfattande område så har en avgränsning gjorts till att endast behandla de externa hot som förekommer i samband med anslutning till Internet.

Denna rapport kommer att utgå från att behandla de externa hot och logiska skyddsåtgärder som tagits upp i kapitel 2. Dessa hot och risker kommer att ligga till grund för den undersökning som skall göras hos olika företag. Detta arbete avgränsas till att undersöka företag från två olika branscher tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag som använder sig utav Internet som en del av deras verksamhet.

På grund av tidsbrist begränsas arbetet till att endast omfatta de externa hot/logiska hot som kan drabba en organisations IT-system vid anslutning till Internet. Rapporten kommer att fokusera sig på de externa hoten och hur dessa kan åtgärdas med hjälp av logiska skyddsåtgärder d.v.s. som är av teknisk karaktär.

Antalet verksamheter kan komma att bli relativt lågt då det kan vara svårt att få tag i IT-säkerhetsansvariga i verksamheter som har tid över att ställa upp för denna undersökning.

3.4 Förväntat resultat

Resultatet förväntas bidra med en ökad förståelse inom ämnet och en kartläggning av de externa hot som anses vara vanligast, samt kunskapen om hur man ska gå tillväga för att åtgärda dessa hot med hjälp av logiska skyddsåtgärder. Hotbilden antas vidare skilja sig åt mellan branscherna/verksamheterna då vissa branscher antas vara mer utsatta för hoten än andra branscher.

4 Metod

I kapitlet beskrivs tänkbara metoder och tillvägagångssätt för insamling av information. Vidare kommer en redogörelse göras på den metod som valts att använda till den problemprecisering som presenterats i kapitel 3.2.

4.1 Angreppssätt

Detta arbete syftar till att undersöka vilken hotbild som finns idag samt vilka skyddsåtgärder som finns för att åtgärda dessa hot. Innan utredningen ska genomföras bör man ta ställning till om ett kvalitativt eller kvantitativt angreppssätt ska väljas. Enligt Patel & Davidson (1994) finns det två synsätt på hur det insamlade materialet skall bearbetas och utvärderas.

Statistik är den vetenskap inom vilken man behandlar olika sätt att kvantitativt bearbeta information. Data samlas in för att sedan ordna, beskriva, bearbeta och analysera med hjälp av vetenskapliga tekniker för att därefter nå kvantitativa resultat (Patel & Davidson, 1994).

Syftet med kvalitativa undersökningar är att skaffa en annan och djupare kunskap än den fragmentiserade kunskap som oftast erhålls vid användning av kvantitativa metoder. Ambitionen är att försöka förstå och analysera helheter. Vid en kvalitativ bearbetning arbetar man oftast med ett textmaterial. En skillnad från kvantitativa undersökningar är att kvalitativa undersökningar använder sig utav löpande analyser, där all bearbetning inväntas tills allt material är insamlat (Patel & Davidson, 1994).

Eftersom detta arbete har som mål att analysera den hotbild som finns samt vilka skyddsåtgärder som finns för att åtgärda dessa hot, anses det kvalitativa angreppssättet mer lämpligt för att uppnå ett bra och korrekt resultat. Den kvantitativa metoden är utesluten eftersom det inte är lika naturligt att mäta de fenomen jag anser undersöka i siffror.

4.2 Möjliga metoder för insamling av information

För att kunna genomföra ett examensarbete måste man ha tillgång till bakgrundsinformation Denna information kan tas fram utifrån olika metoder för att besvara den problemprecisering som presenterats i kapitel 3.2.

De metoder som är relevanta för att besvara problemställningen presenteras nedan.

- Litteraturstudier
- Intervjuteknik
- Enkätundersökning

4.2.1 Litteraturstudie

En litteraturstudie är en systematisk granskning av ett problem med hjälp av att analysera publicerade källor, med ett specifikt syfte i åtanke (Berndtsson m.fl., 2002). Enligt Dawson (1999) är litteratur presenterad i ett antal format. De vanligaste källorna där vi hämtar kunskap hämtas är böcker, artiklar, publicerade i vetenskapliga tidskrifter samt rapporter (Patel & Davidsson, 1994). Vissa format är mer tillgängliga än andra och andra mer kända för att vara mer ’akademiska’ värdefulla (Dawson, 1999). För att få en god inblick i det valda problemområdet (se kapitel 3.2) kan denna typ av litteratur vara lämplig.

Den litteratur som behövs kan man få genom att söka i biblioteken, med hjälp av olika hjälpmedel t ex kataloger och tidskriftssamlingar. Internet kan också vara ett alternativ för att söka efter artiklar och information. Sökning på Internet är inte alltid säker vid insamling av information till ett arbete (Dawson, 1999).

Nackdelen med litteraturgenomgången är att denna typ av studie är en relativ tidskrävande process. Förutom att det är en tidskrävande process så är det inte säkert att den litteratur som behövs finns tillgänglig, p.g.a. att litteraturen är utlånad eller kanske inte finns på just det biblioteket och måste därför göra ett fjärrlån. Slutligen måste man gå igenom litteraturen som lånats som är ännu en tidskrävande process, därför är det viktigt att ta med detta i beräkningen med andra ord tidsplaneringen när undersökningen ska påbörjas.

En annan nackdel med litteraturstudier är enligt Berndtsson m.fl. (1999) svårigheten att veta när tillräcklig med material har samlats in. Med andra ord när man bör sluta samla in material. Det viktigaste är att arbetet har en hög validitet, d.v.s. hur läsaren finner innehållet i rapporten trovärdig (Berndtsson m.fl., 2002). Genom att använda sig utav en systematisk process och strategi för att samla in tillräcklig material som ska förmedlas till läsaren, finns en större chans att läsaren kommer att förstå och uppskatta strategierna och kommer då att kunna förlita sig på den tillräckliga informationen.

Genom att använda sig utav litteraturstudier för att utreda arbetets problemställning, finns det möjlighet att ge en ökad kunskap och insikt i problemområdet. Litteraturen inom området externa hot vid anslutning till Internet räcker inte till för att besvara examensarbetets problemställning. Genom att läsa litteratur som behandlar problemställningen skulle en slutsats kunna dras om vad just litteraturen säger, men för att få en bild av vilken hotbild olika företag har samt hur de väljer att skydda sig mot hoten räcker inte en litteraturstudie.

4.2.2 Enkätundersökning

En annan teknik för att samla in information på ett snabbt och billigt sätt är enkätundersökningar som bygger på frågor (Patel & Davidson, 1994). Formuleringen av frågorna är viktig för att man ska kunna minska mångtydigheten och få tillräckligt precisa frågor så att svarspersonerna förstår vad som menas med frågorna (Bell, 1995). Vidare ska det bestämmas vilken typ av frågor som ska användas och försäkra sig om att man kommer att kunna kategorisera och analysera svaren.

Vid enkäter är det viktigt att det framgår om deltagandet är anonymt eller ej. Om en enkät är anonym, finns varken namn, nummer eller annan möjlighet till identifiering på den. Detta medför att vi inte kommer att veta vem som svarat i dessa enkäter och vid behov måste påminnelser skickas till samtliga deltagare. Är enkäten konfidentiell innebär det att vi vet vem vi har fått svar från men att det bara är vi som har tillgång till de uppgifterna. Påminnelser skickas då bara till dem som inte har besvarat enkäten. Det är även viktigt att namnlistan förstörs så att inte någon kan identifiera vem som besvarat en viss enkät hävdar Patel och Davidson (1994).

Enligt Patel och Davidsson (1994) kan enkäter indelas i ostrukturerade och strukturerade. Vid användning av frågor med fasta svarsalternativ, är dessa frågor helt *strukturerade*. En ostrukturerad enkät innehåller öppna frågor d v s frågor utan fasta svarsalternativ vilket innebär att den tillfrågade själv kan formulera sina svar. Vissa frågor kan formuleras så att det bara blir möjligt att svara t ex ”ja” eller ”nej” som i detta fall blir en strukturerad fråga (Patel & Davidson, 1994). Frågor kan även formuleras så svarsutrymmet lämnas fritt, t ex ”Vad anser du om…”. Beroende av hur man väljer att kombinera grad av standardisering och grad av strukturering så får vi olika typer av enkäter som har olika användningsområden (Patel & Davidsson, 1994).

Enkäter är ett lättare alternativ för att ställa mer känsliga och ledande frågor än vid en intervju. Detta kan bero på att det kan ses som känsligt att ställa vissa typer av frågor vid personlig kontakt med respondenten. Man måste vara väldigt noggrann när det gäller formulering och var i enkäten man sätter de känsliga frågorna (Bell, 1995). Ett alternativ är att ha de känsliga frågorna bland de sista frågorna som ställs i enkäten, med tanke på att svarspersonen annars väljer att inte fullfölja enkäten. Eftersom åldern kan betraktas som en känslig sak att fråga om kan man istället använda sig utav kategorier med vissa åldersintervall som kan kryssas i (Bell, 1995).

Det blir alltid ett större eller mindre bortfall, därför ska man i förväg bestämma sig för hur lång tid det ska gå innan man kan skicka ut en påminnelse. Man bör alltid anstränga sig för att göra bortfallet så litet som möjligt, dvs i så stor utsträckning som möjligt motivera personerna att besvara och skicka tillbaka enkäterna. Nackdelen är att det tar lång tid att sammanställa enkäterna (Bell, 1995). Fördelen med att använda en enkätundersökning är att man kan nå många personer på ett enklare sätt. En intervjuundersökning är tidskrävande samt att man inte kan nå lika många personer vilket leder till ett större bortfall.

Genom att använda sig utav enkäter för att utreda vad företag har för extern hotbild samt vilka skyddsåtgärder de väljer för att åtgärda hoten., ges en möjlighet till att nå många personer på ett enklare, snabbare och billigare sätt. Detta kan ses som en fördel då examensarbetet ska utföras under en tidsbegränsad tid. Eftersom undersökningen består utav frågor med fasta alternativ kan en strukturerad enkät ses som ett alternativ till undersökningen. Detta minskar risken för respondenten att inte svara på frågorna. Nackdelen med att använda enkäter för att ta reda på vilka externa hot som anses vara vanliga samt vilka skyddsåtgärder som används är den att det inte går att diskuttera problemområdet öppet vilket är en förutsättning för att uppnå ett bra resultat.

4.2.3 Intervju

Intervju är en annan teknik som kan ligga till grund för att besvara det preciserade problemet som återfinns i kapitel 3. Intervju är en teknik som används för att samla in information som bygger på frågor (Patel & Davidson 1994). Syftet med intervjuteknik är att lära sig att söka information inom ett sak- eller problemområde, att lära sig vara öppen, lyhörd och fördomsfri. Respondentens svar kommer att utgöra data som efter analys kommer att ge ett resultat vilket ligger till grund för en slutsats eller ett beslut. Respondentens svar måste därför ha en tillförlighet som gör det möjligt att dra en ”säker” slutsats och det måste vara möjligt att kritiskt granska resultaten (Lantz, 1993).

Vid insamling av information är det två aspekter som bör beaktas, skriver Patel och Davidson (1994). Dels är det frågornas utformning och inbördes ordning vilket kallas grad av *standardisering* och dels graden av *strukturering*. Med grad av strukturering innebär i vilken utsträckning frågorna är fria för intervjupersonen att tolka fritt. När det gäller grad av standardisering innebär det att vid helt standardiserade intervjuer ställs likvärdiga frågor i samma ordning till varje respondent (Patel & Davidson, 1994). Standardiserade intervjuer används oftast när man vill kunna jämföra samt generalisera information. När det gäller grad av strukturering handlar det om vilket svarsutrymme intervjupersonen får. En helt ostrukturerad intervju är helt öppen, vilket innebär att intervjuaren ställer en vid, öppen fråga som intervjupersonen fritt kan utveckla sina tankar kring (Lantz, 1993).

Ju mer standardiserad intervjun är, desto lättare är det att ordna och kvantifiera resultaten. Om en intervju inte är standardiserad kan frågorna formuleras under tiden intervjun pågår och de anpassas till respondenten. En strukturerad intervju kan likna en enkät. De flesta intervjuer som görs under informationsinsamlingsfasen brukar hamna mellan den strukturerade och den helt ostrukturerade intervjun. Att ge respondenten frihet att prata om det som är viktigt för honom/henne är förstås av stor betydelse, men en viss struktur i intervjun är också av stor vikt (Bell, 1995).

Patel & Davidson (1994) skriver att eftersom intervjuer bygger på frågor är intervjuaren hänvisad till individens villighet att svara på frågor. Det är därför viktigt att försöka motivera dessa personer att svara på frågorna på bästa möjliga sätt. Genom att förklara syftet med intervjun och i största möjliga utsträckning relatera syftet till individens egna mål kan vilja svara på intervjufrågor öka för personen ifråga. Det är även viktigt att betona individens roll i sammanhanget och vad informationen kommer att användas till. Enligt Berndtsson m.fl. (2002) kan en öppen intervju innebära en nackdel genom att intervjun kan bli komplicerad för oerfarna intervjuare.

Vid användning av intervjuteknik minskar risken för att frågor inte kommer att bli besvarade av respondenterna, bl a genom att respondenten har möjligheten att ifrågasätta frågor som ses som otydliga på plats samt att risken för bortfall inte kommer att bli så stort. Dessa punkter leder till att projektarbetets undersökning kan utföras på ett sätt att frågorna besvaras på ett tydligare sätt och genom att motivera respondenten kan alla frågor besvaras, vilket leder till att bortfall minskas och att resultatet blir säkrare.

En stängd intervju karaktäriseras av ett bestämt antal frågor, som intervjuaren ställer till varje person i undersökningen. Denna intervjuform är mer vanligt förekommande i kvantitativ forskning, där det används statistiska metoder för att analysera resultat.

Genom att använda sig utav intervjuer för att utreda arbetets problemställning, ger detta en möjlighet till att förtydliga frågor och svar som ges i samband med intervjuerna vilket leder till i alla fall minimera risken för att inga missförstånd uppstår bland frågor och svar. En intervju ger respondenten möjlighet att förstå syftet med undersökningen på ett bra och tydligt sätt genom att ställa öppna frågor till intervjuaren. Detta leder till att respondenten får en ökad förmåga att svara på frågorna. En öppen intervju är enligt Berndtsson m.fl. (2002) en form av intervju som används vid kvalitativa undersökningar.

Vid användning av intervjuteknik minskar risken för att frågor inte kommer att bli besvarade av respondenterna, bl a genom att respondenten har möjligheten att ifrågasätta frågor som ses som otydliga på plats samt att risken för bortfall inte kommer att bli så stort. Dessa punkter leder till att projektarbetets undersökning kan utföras på ett sätt att frågorna besvaras på ett tydligare sätt och genom att motivera respondenten kan alla frågor besvaras, vilket leder till att bortfall minskas och att resultatet blir säkrare.

4.3 Val av metod

I detta kapitel presenteras vilken metod som kommer att användas för att utreda problemställningen i arbetet.

Valet av metod för att undersöka vilken extern hotbild verksamheterna har i samband med anslutning till Internet samt hur de väljer att åtgärda dessa hot var relativt enkelt. För att lösa frågeställningen för detta examensarbete väljs att göra intervjuer Detta anses vara det mest lämpade angreppssättet vid studier av vilken hotbild verksamheterna har i samband med Internet samt vilka skyddsåtgärder de väljer att använda för att åtgärda de externa hoten. Intervjutekniken anses vara det mest lämpade angreppssättet i denna undersökning då den personliga kontakten skulle underlätta då intervjufrågorna bör vara av öppen karaktär och kan behövas diskuteras med intervjupersonen. Det är nödvändigt att ge intervjupersonen stor frihet i vissa svar för att få omfattande svar på vilken extern hotbild företaget har i samband med anslutning till Internet samt hur vilka skyddsåtgärder som de väljer att använda för att åtgärda hoten. Är de intervjuade låsta till vissa angivna hot och skyddsåtgärder blir resultatet av undersökningen inte rättvisande.

För att genomföra denna undersökning hos företagen är det viktigt att frågorna uppfattas på samma sätt av alla respondenter samt att eventuella oklarheter i frågor kan förklaras vilket kan göras vid en intervju med tanke på den personliga kontakten. Intervjufrågorna ligger till grund till examensarbetets problemprecisering och är därför väldigt viktigt att frågorna uppfattas på korrekt samt att respondenten får möjlighet att besvara frågan öppet för att uppnå ett bra resultat av detta examensarbete. Vid intervjuer får respondenten även möjlighet att ställa följdfrågor för att utveckla svaren ytterligare.

Detta examensarbete kräver en kvalitativ undersökning för att besvara frågeställningen därför ses besöksintervjuer som den bäst lämpade tekniken för att lösa uppgiften. Intervjuerna kommer att utföras med hjälp av strukturerade frågor med hög grad av standardisering. Intervjun kan ses som en stängd intervju då undersökningen kommer bestå utav ett antal bestämda frågor som respondenten kan svara öppet, frågorna kan ses som öppna frågor. Intervjuerna skall förhoppningsvis ge utförliga svar med hög kvalité samt vara av samtals- och diskussionstyp, därmed är enkät inte lämpligt. Syftet med att utföra en kvalitativ undersökning är att skapa en djupare förståelse för den externa hotbild som företagen har i samband med anslutning till Internet samt hur de väljer att åtgärda dessa hot. Besöksintervjuer är tidskrävande och kan innebära en begränsning i valet av respondenter till ett begränsat geografiskt område.

För denna undersökning kommer varje respondents svar behandlas konfidentiellt. Varje respondent kommer att benämnas med R och ett nummer, exempelvis R1 o s v. Tanken är att besöksintervjuer skall ge svar på frågeställningen, dock kan det bli nödvändigt att i vissa fall utföra intervjun med hjälp av telefon på grund av geografisk spridning av intervjuobjekten.

Intervjuerna är tänkta att utföras som besöksintervjuer i den mån det är möjligt och i övriga fall kommer telefonintervju att göras. Att besöksintervjuer väljs framför någon typ av enkät är att den personliga kontakten med respondenten är önskvärd i detta arbete. Telefonintervjuer är svårare att dokumentera med hjälp av bandspelare, då det kräver högtalartelefon. Dels kan det vara lättare att missförstånd uppstår då kroppsspråk och mimik inte kan uppfattas vid telefonintervjuer. Ytterligare en anledning till att besöksintervjuer valts framför enkäter är fördelen med att få igång en eventuell diskussion vid intervjuerna.

Enkäter var inte ett bra angreppssätt på just detta problemområde då det inte är aktuellt med en statistisk undersökning. En enkät där intervjupersonen själv får svara öppet på frågorna skulle vara mycket svårt att utföra. Detta skulle bli mycket tidskrävande för intervjupersonen och det skulle vara komplicerat att formulera tillräckligt tydliga frågor. Enkäter kan vara bra om undersökningen skulle innefatta ett flertal respondenter, men så är inte fallet då undersökningen endast ska bestå utav ett fåtal respondenter.

Litteraturstudier har valts att användas vid insamling av bakgrundsfakta där litteraturen behandlar de externa hot som förekommer vid anslutning till Internet samt vilka skyddsåtgärder som används för att åtgärda dessa hot. Denna litteraturstudie ska ligga till grund till intervjuns struktur för att se om verkligheten stämmer överens med litteraturen.

Att använda intervjutekniken för att förvärva information från respondenterna synes som mest lämpligt för att få utförliga svar på frågorna i denna relativt begränsade undersökning.

4.4 Intervjuernas upplägg

Nedan redovisas hur intervjuerna lagts upp och utförts. Dessutom beskrivs hur intervjupersonerna valts ut och frågorna beskrivs och motiveras.

4.4.1 Intervjuernas utförande

Svaren, från besöksintervjuer kommer att spelas in på band och antecknas. Anledningen till båda metoderna används är dels att det finns en backup ifall inspelningen skulle misslyckas och dels kan anteckningarna förtydliga vilka delar av svaren som verkat mest angeläget hos intervjupersonen vid själva intervjutillfället. Vid en möjlig telefonintervju kommer svaren endast att antecknas då det inte finns någon möjlighet till en högtalartelefon. Intervjuerna kommer att utföras på intervjupersonens arbetsplats i de fall det är möjligt då det ger en mer avslappnad situation. Varje intervju beräknas ta cirka fyrtio minuter.

4.4.2 Undersökningsgrupp

Vid planeringen av intervjuerna har ett önskemål satts upp om att mellan tre och fem intervjuer ska utföras. De urvalskriterier som finns för företagen är att de skall arbeta med Internet på ett eller annat sätt. Urvalet sker även geografiskt för att intervjuerna skall kunna utföras på intervjupersonens arbetsplats. Urvalskriterierna för intervjupersonerna är att de har kunskap om IT-säkerheten inom företaget. Kön, ålder och erfarenhet tas ingen hänsyn till då antalet möjliga intervjupersoner inte är tillräckligt stort för att jämföras.

4.4.3 Inledande information till intervjupersonerna

Vid den första kontakten med företagen har en del information angående examensarbetets utformning och syfte förberetts. Detta för att dels ge en bild av vad som efterfrågas och dels för att kontrollera att rätt person kontaktas. När tid för intervju bestämts sänds ytterligare information med en kort introduktion till frågeställningen och exempel på frågor som kan ingå i intervjun för att ge intervjupersonen en chans att förbereda sig något. Den information som skickats finns presenterad i bilaga 1. Respondenten får en möjlighet att sätta sig in i frågorna och på så sätt undvika att respondenten avger snabba och ytliga svar.

4.4.4 Intervjufrågor

Utformningen av intervjufrågorna gjordes utifrån de fakta som inhämtats i arbetet med rapportens bakgrund tillsammans med problemställningen. De frågor som till slut verkade aktuella för att ge svar på problemställningen sammanställdes i en ordning som innebar att svaren inte skall påverkas av tidigare frågor.

Intervjuerna har lagts upp så att de intervjuade personerna skall svara på frågorna i den ordning de följer, varje fråga ska kunna diskuteras öppet.

Totalt består intervjun av åtta frågor som respondenten skall besvara. Intervjun inleds med ett antal allmänna frågor om intervjupersonen och företaget i fråga. Dessa allmänna frågor handlar om respondentens erfarenhet och befattning. Dessutom ställs en fråga om företagets arbete med Internet. Syftet med de allmänna frågorna har varit dels att få en bild av intervjupersonen och företaget och dels har det varit ett sätt att mjukstarta intervjun. Att få en bild av företaget kan underlätta analysen av utfallet på intervjufrågorna..

Efter de allmänna frågorna ställs frågor om företagets externa hotbild vid anslutning till Internet och vilka av de nämnda skyddsåtgärder i intervjun som används för att åtgärda hoten. Intervjun avslutas med att övriga frågor som kommit upp under intervjun kan ställas.

Nedan redovisas och motiveras de frågor som ingått i intervjun:

1. *Vad är ditt namn och vad är din befattning?*

Denna inledande fråga kontrollerar intervjupersonens namn och intervjupersonens nuvarande befattning fastställs för att säkerställa att intervjupersonen stämmer överens med urvalskriterierna.

2. *Hur många år har du arbetat på företaget?*

Intervjupersonens erfarenhet på det aktuella företaget är intressant att se för att se om de följande svaren skiljer sig mellan mer eller mindre erfarna intervjupersoner.

3. *Ge en kort beskrivning av vad företaget använder Internet till.*

Denna fråga ger en överblick över vad företaget arbetar med vid en anslutning till Internet. Eventuella likheter och skillnader uppmärksammas för att senare jämföras.

4. *Har ni en fast anslutning till Internet?*

Det är i detta arbetet intressant att veta vilken anslutning företaget har till Internet, för att analysera de hot som kan komma att drabba företaget.

5. *Ser Ni några risker med att företaget är anslutet till Internet? Varför?*

6. *Vilken hotbild är vanlig i förhållande till Ert IT-system vid anslutning till Internet vad gäller nedanstående hot? Har nedanstående hot någon gång förkommit eller drabbat Ert IT-system? Hur tror Ni att hotbilden ser ut generellt?*

   a) Virus
   b) Hackers
   c) Obehörig åtkomst genom att skaffa användaridentitet och lösenord
   d) Åtkomst av känslig information i form av modifiering, tillägg eller borttagning av information.
   e) Ändra innehåll på webbsidor
   f) Risk för avlyssning av meddelanden inom företaget

Denna fråga ligger till grund till min problemprecisering. Detta svar ska jämföras med den hotbild kapitel 2 tar upp.

7. *Vad anser Ni vara det största externa hotet mot Ert IT-system med tanke på anslutning till Internet?*

Frågan ställs för att säkerställa vad företaget anser vara det största hotet.

8. *Vilka tekniska skyddsåtgärder används bland **kryptering, behörighetskontrollsystem, brandvägg och antivirusprogram** för att åtgärda möjliga hot som kan drabba Ert företag vid anslutning till Internet? Vid användning av nämnda skyddsåtgärder kan fråga 8a ställas och om inget användande av respektive skyddsåtgärd används ställs fråga 8b.*

   a) *Varför används just denna skyddsåtgärd och till vilket syfte?*
   b) *Varför har Ni valt att inte använda Er utav denna skyddsåtgärd?*

Denna fråga ligger till grund till min problemprecisering. Hur väljer företaget att skydda sig mot de externa hoten?

9. *Övriga frågor?*

Möjlighet att ställa övriga frågor som kommer upp under intervjun.

5 Genomförande

I detta kapitel kommer en beskrivning ske angående hur undersökningen genomfördes och hur intervjuprocessen var. Dessutom ingår ett avsnitt om erfarenheter och problem under genomförandet.

5.1 Intervjuförberedelser

När beslut tagits att undersökning skulle ske med hjälp av intervjuer inleddes arbetet med att kontakta företag. I de flesta fall var personen som kontaktades en systemadministratör eller en IT-ansvarig. De tänkbara intervjupersonerna fick en kort introduktion till arbetet vid det första telefonsamtalet då även tid för intervju bestämdes. Innan intervjun skickades ett introduktionsbrev till respondenterna via e-post, se bilaga 1. I detta brev informerades de om examensarbetets frågeställning. De fick två öppna frågor att börja fundera på innan själva intervjun.

Tyvärr gick det inte alltid så bra då man kopplades från den ena personen till den andra, samt att personen inte kunde kontaktas under en längre period, vilket ledde till att ett annat och annat företag kontaktades. Till en början var det två intervjuer inbokade och intervjuprocessen blev något utdragen. Efter en mer omfattande sökande efter respondenter hittades tre till som var villiga att bidra med sina åsikter om externa hot och skyddsåtgärder för att åtgärda hoten. Sammanlagt bokades fem stycken intervjuer.

Innan intervjun skulle genomföras hos företag utfördes den tänkta pilotintervjun på två elever på Högskolan i Skövde. Pilotintervjun gav en erfarenhet av intervjusituationen och en genomgång av intervjufrågorna. Pilotintervjun gick bra och inga korrigeringar behövde göras bland intervjufrågorna.

5.2 Besöksintervju

De företag som kontaktats och som ställt upp för besöksintervju är fyra till antalet. De respondenter som var möjliga att intervjua bokade sin tid att medverka i intervjun redan vid första telefonkontakten. I första hand var detta introduktionsbrev tänkt att skickas till respondenter där en intervju var mest lämpat, men för att samtliga respondenter skulle få samma förutsättningar beslutades att även respondenterna i besöksintervjuerna skulle få detta introduktionsbrev. Besöksintervjuerna genomfördes på respondenternas arbetsplatser. Intervjuerna inleddes med ett litet samtal och respondenten tllfrågades om de accepterade att intervjun dokumenterades på band. Eftersom området IT-säkerhet är ett väldigt känsligt område att diskutera om användes inte bandet vid alla intervjuerna. Besöksintervjuerna tog emellan ½ till 1 timma. Samtliga respondenter svarade på frågorna med en del kompletterade med mycket information runt ämnet. En orsak till varför en del intervjuer blev väldigt korta kan vara att respondenten svarade kort och koncist på frågorna utan att beskriva sammanhanget så ingående. Alla intervjuade personen har varit mycket tillmötesgående och verkade positivt inställda till intervjun. Den planerade intervjutiden hade uppskattats till drygt 40 minuter och den genomsnittliga intervjun blev cirka 40 minuter.

5.3 Telefonintervju

Efter att kontakt tagits med respondenten via e-mail skickades svar när de önskade bli uppringda. Respondenten var mycket tillmötesgående. Intervjun kunde inte dokumenteras med hjälp av bandspelare eftersom intervjun inte gjordes från en högtalartelefon. Det var relativt lätt att få respondenten att svara omfattande på frågorna. Telefonintervjun gick ganska lätt att utföra och respondenten var prat glad och delgav mycket information. Den telefonintervju som genomfördes var cirka 30-40 minuter lång. Intervjuernas olika tidsåtgång vid både besöksintervjuerna och telefonintervjun kan förklaras med skillnaden i informationsgivningen runt omkring frågorna.

5.4 Bearbetning av intervjusvar

Efterhand som intervjuerna avklarades sammanställdes svaren från anteckningarna samt bandupptagningen som användes vid vissa intervjuer. Intervju svaren redovisas i kapitel 6.2.

5.5 Erfarenheter och problem

Respondenterna ville gärna hjälpa till vid intervjuerna och därför svarade de väldigt utförligt på frågorna. Frågekonstruktionen var ett komplext område som innebar mycket funderande och justerande. Frågorna förändrades efter första pilotintervjun. Bedömningen som gjordes efter den första pilotintervjun, var att det var viktigt att använda samma frågor till samtliga respondenter.

Att använda sig utav bandinspelning för dokumentation har setts som en stor fördel. Respondenterna har i nästan samtliga fall inte tvekat om att godkänna banddokumentationen av intervjuen.

Respondenterna har svarat utförligt på frågorna. Ibland har de kanske varit lite omfattande så man hamnat utanför ämnet men detta är något som positivt uppskattats. Dock har författaren vid genomgången av dokumentationen efter intervjun funnit att alla frågor vid några fall inte blivit besvarade.

Av olika omständigheter blev sökandet efter intervjuobjekt försenat. Några av orsakerna till att det blev försenat var att de tillfrågade inte kunnats nå på grund av exempelvis de har varit på tjänsteresa.

5.6 Värdering av det insamlade materialet

I det insamlade materialet ingår intervjusvar från fem olika respondenter. Två respondenter representerar svar från branschen tjänsteföretag som arbetar med elektroniska penningstransaktioner och tre respondenter representerar svar från övriga tjänsteföretag. Eftersom respondenterna som intervjuades har stor kunskap inom området IT-säkerhet blir det insamlade materialet relativt representativt för den organisationen där intervjun genomförts. I urvalsprocessen för denna undersökning har i stort sätt samtliga respondenter ett arbete som berör IT-säkerheten. Undersökningen har inte så stor geografisk spridning

majoriteten av respondenterna är från Jönköping och endast en från Stockholm. Intervjusvaren var mycket omfattande men all insamlad information är inte relevant för att besvara frågeställningen. Materialet skulle sannolikt vara ännu mera intressant om ytterligare intervjuer genomförts och då inom olika organisationer, men då det insamlade materialet kommer från användare med olika bakgrund, erfarenhet kan materialet användas för analys och för att besvara frågeställningen för detta examensarbete.

6 Materialpresentation

I detta kapitel redovisas svaren från intervjuerna. Svaren från verksamheterna har sammanställts och skickats till respektive respondent för verifiering. Verifiering har gjorts för att kontrollera att inga misstolkningar gjorts i resultat och detta anses öka resultatets tillförlitlighet.

6.1 Respondenternas verksamhet

Nedan presenteras de företag som deltagit i examenarbetets undersökning.

6.1.1 Länsförsäkringen Bank

Det första ömsesidiga lokala länsförsäkringsbolaget bildades år 1801. Idag består Länsförsäkringen av 24 självständiga och lokala länsförsäkringsbolag som samverkar genom det gemensamt ägda Länsförsäkringar AB med dotterbolag. Tillsammans skapar dessa länsförsäkringsbolag, Sveriges enda kundägda och lokalt förankrade bank- och försäkringsgrupp.

Länsförsäkringar erbjuder ett komplett sortiment av bank och försäkringstjänster. Bland dessa är banksparande, fondsparande, lån, bankkort, livförsäkring, pensionsförsäkring, hemförsäkring, villaförsäkring, olycksfallsförsäkring, industriförsäkring, trafikförsäkring samt djurförsäkring.

6.1.2 Kitron Development

Kitron ASA är en ledande nordisk koncern inom området kontraktsutveckling och produktion av elektronikprodukter med totalt c:a 1700 anställda. Koncernen har i Sverige 3 bolag, Kitron Electronics, Kitron microelectronics, Kitron Development.

Kitron Development AB är ett konsultbolag som bedriver försäljning av tekniska tjänster främst inom elektronikutveckling. Kompetens finns även inom området systemutveckling, inom affärsområdet SoftTech. Kitron Development har identifierat ett ökat behov på marknaden av mjukvarutjänster, och avser därför att expandera på detta område. Starka kompetenser finns inom områden som databasdrivna Webbapplikationer, testsystem och embedded systems.

6.1.3 SEB

SEB-koncernen är en nordeuropeisk finansiell bankgrupp för företag, institutioner och privatpersoner. SEB har totalt 672 kontor i Sverige, Tyskland och Baltikum och över 4 miljoner kunder, varav 1,5 miljoner Internetkunder. Koncernen finns representerad i ett 20-tal länder jorden runt och har cirka 19.000 anställda.

SEB är en ledande finansiell partner i Norden med en stark europeisk närvaro och internationell räckvidd. SEB utgör en naturlig samarbetspart för såväl privatpersoner som företag, i allt från att förenkla vardagsekonomi till rådgivning i komplicerade företagsaffärer.

6.1.4 Kapsch TrafficCom AB (f d Combitech Traffic Systems AB)

Kapsch TrafficCom AB (f d Combitech Traffic Systems AB) bildades 1992 under SAAB Aerospace men såldes i mars 2000 till österrikiska telecomkoncernen Kapsch AG. Kapsch TrafficCom AB har drygt 30 procent (undantaget USA) av världsmarknaden på elektroniska vägtullsystem, de flesta i Fjärran Östern och Australien. Koncernen har ca 90 anställda varav ett 10-tal arbetar på dotterbolag i Australien, Chile och Malaysia. Dessutom finns representationskontor i Kina och Sydafrika.

Kapsch TrafficCom AB är världsledande med tredje generationens helautomatiska system för upptagning av vägavgifter. Systemen används idag av över 4,5 miljoner bilister i 22 länder. Marknaden har inga tydliga gränser, kontor finns i världsstäder från Melbourne i Australien och Kuala Lumpur i Malaysia till Guangzhou i Kina, Johannesburg i Sydafrika och Santiago i Chile. Huvudkontoret ligger i Jönköping med ca 100 anställda, där sker produktutveckling och där finns även deras testanläggning

6.1.5 SYSteam

SYSteam arbetar dels som bred IT-Partner till små- och medelstora företag och dels som specialist inom ERP, Utveckling och Management till större företag. SYSteam är etablerat med kontor och dotterbolag på 48 orter i Norden. Koncernen har idag ca 1000 anställda. SYSteam har idag ca 3800 kunder, varav 2300 är affärssystemkunder.

6.2 Redovisning av insamlade intervjusvar

Nedan följer redovisningen av respondenternas svar. Redovisningen av svaren delas in i fyra avsnitt (A, B, C, D). I varje avsnitt redovisas vid varje fråga respondenternas svar. Intervjufrågorna finns med i bilaga 2. Materialet är uppdelat i följande avsnitt:

A. Respondentens tidigare erfarenhet och dennes trovärdighet inför denna undersökningen.
B. Verksamhetens användning av Internet och syn på risker med Internetanslutning.
C. Verksamhetens externa hotbild vid anslutning till Internet.
D. Skyddsåtgärder verksamheten valt att använda och till viket syfte.

A. Respondentens tidigare erfarenheter och deras trovärdighet inför intervjuerna

- *Vad är din befattning och hur många år har du arbetat inom detta område?*

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 arbetar som *IT-ansvarig* och har arbetat inom detta område i ca *åtta år*. R1 berättar att denne har en god kunskap

inom IT-säkerhet och kunskap om externa hot och skyddsåtgärder.

SEB: R3 arbetar som Informationssäkerhets chef på IT-kontoret i Stockholm och har arbetat i denna position i 3 år.

Övriga tjänsteföretag

Kitron Development: R2 har i *fem år* arbetat som systemadministratör och även tagit en magisterexamen inom dataingenjörsprogrammet. R2 berättar vidare att *" en del av mitt arbete går ut på att kontrollera IT-säkerheten inom verksamhetens IT-system, exempelvis genom att kontrollera trafiken i systemet*".

Kapsch TrafficCom AB: R4 har i tre år arbetat som IT-ansvarig och har fått sin Erfarenhet från tidigare jobb samt sin magisterexamen inom dataingenjörsprogrammet.

SYSteam: R5 arbetar som IT-säkerhetsanvarig och har arbetat i denna position i 2 år. R5 har arbetat inom IT-branschen i 8 år.

B. Verksamhetens användning av Internet och syn på risker med Internetanslutning.

- *Ge en kort beskrivning av vad företaget använder Internet till?*

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 berättar att Internet är ett praktiskt redskap för verksamheten. R1 menar på att Internet kan vara till stor hjälp för att utföra verksamhetens arbetsuppgifter. Internet används bl.a. mycket till att skicka e-post med. R1 talar även om att verksamheten jobbar mycket mot World Wide Web när information och uppgifter behöver hämtas för ett arbete.

SEB: R3 svarade att Internet till stor del används för att ta kontakt med omvärlden. R3 förklarade också att många av verksamhetens tjänster erbjuds via Internetbanken där Internet används flitigt.

Övriga tjänsteföretag

Kitron Development: R2 beskriver Internet som ett hjälpmedel för att kunna utföra en del av verksamhetens arbetsuppgifter. Verksamheten

använder Internet bl a för att hämta information om företag och produkter, ladda ner olika program, program för att uppdatera virusprogram.

Kapsch TrafficCom AB: R4 svarade att Internet används till många syften bl.a som en extern site där företaget lägger ut dokument som leverantörerna kan hämta. Internet kan användas för att lägga ut information med andra ord kan en del av marknadsföringen göras genom Internet menade R4. R4 svarade vidare att Internet används internt inom verksamheten vid e-post, informationssökning (surfning) vid problemlösning.

SYSteam: R5 beskriver Internet som ett hjälpmedel som används till det mesta. Felanmälan från kunder samt distansarbete utförs med hjälp av Internet.

- *Har Ni en fast anslutning till Internet?*

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 svarade ”*Ja”* och menar på att en fast anslutning behövs då Internet används i stor utsträckning i verksamheten.

SEB: R3 svarade ”Ja” och menade på att en fast anslutning är behövlig eftersom Internet används dagligen i verksamheten.

Övriga tjänsteföretag

Kitron Development: R2 svarade att verksamheten använder sig utav en fast anslutning till Internet.

Kapsch TrafficCom AB: R4 svarade att verksamheten använder sig utav en fast anslutning via en extern leveratör som ansvarar för uppkopplingen.

SYSteam: R5 svarade att “Ja” på frågan och berättade att verksamheten har en 10 Mb/s anslutning till internet.

- *Ser Ni några risker med att företaget är anslutet till Internet? Varför?*

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 svarade att det finns en självklar risk med att koppla upp sig mot Internet. R1 menar på att genom att vara ansluten till Internet öppnas vägar för utomstående att skada verksamhetens system som kan påverka verksamhetens effekt av arbetsuppgifter. R1 berättade att verksamheten är fullt medveten om riskerna som kan förekomma i samband med en anslutning till Internet och arbetar fullt för att förebygga dessa risker exempelvis genom en genomtänkt säkerhetspolicy.

SEB: R3 svarade att det klart finns en hot och riskbild i samband med en anslutning till Internet, och förklarade att de arbetar för att förebygga hoten och riskerna med hjälp av olika skyddsåtgärder.

Övriga tjänsteföretag

Kitron Development: R2 svarade att verksamheten ser en självklar risk med att vara ansluten till Internet och säger att helst skulle man vara utan. Men eftersom Internet är ett viktigt redskap för arbetet behövs Internet och verksamheten satsar stort för att förebygga riskerna som kan förekomma.

Kapsch TrafficCom AB: R4 svarade att säkerhetsrisken självklart finns i samband med en anslutning till Internet. Förutom den direkta säkerhetsrisken finns det även en indirekt i form av effektivitetssänkning dvs genom att vara ansluten till Internet finns risken att systemets effektivitet kan sänkas svarade R4 och låta medarbetare surfa kan kan man råka ut för eventuell ”surfmissbruk” som i sin tur sänker effektiviteten hos den anställde.

SYSteam: R5 svarade att det definitivt finns en risk med att vara ansluten till Internet och som måste värderas. R5 menade på att Internet är globalt och öppnar många vägar för en utomstående att hacka sig in i systemet.

C. Verksamhetens externa hotbild vid anslutning till Internet.

10. Vilken hotbild anser Ni vara vanlig i förhållande till Ert IT-system vid anslutning till Internet vad gäller nedanstående hot? Har nedanstående hot någon gång förkommit eller drabbat Ert IT-system? Hur tror Ni att hotbilden ser ut generellt?

- Virus

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar:

R1 svarade att virus ofta fastnar i bolagets virusskydd vid inkommande mail från avsändare utanför bolaget, men har inte drabbat systemet på så sätt att effekten på systemet påverkats.

R1 menar på att virus är väldigt vanligt i samband med e-post. Vidare sades det att verksamhetens policy är till stor hjälp vid situationer då exempelvis ett virus skulle uppstå. Policyn talar då om hur användaren ska gå till väga för att åtgärda viruset. R1 svarade också med att företaget försöker uppmana användarna av systemet att inte klicka på vad som helst. R1 förklarade att virus är ett hot som förekommer ofta men som inte drabbat verksamheten.

Generellt sett ser R1 virus som ett ofta förekommande hot som kan påverka ett verksamhets system om inte skyddsåtgärder och policyn används. R1 ville påpeka att verksamheten även klassar kedjebrev som ett virus, men det är inget som förekommer ofta.

SEB:

R3 svarade att virus är ett vanligt förekommande hot men eftersom företaget har säkra skyddsåtgärder för detta hot har systemet inte påverkats på något sätt. R3 ansåg även att virus generellt kan ses som ett självklart hot som kan förekomma dagligen.

Generellt sett tyckte R3 att virus är ett vanligt förekommande hot som kan påverka tillgängligheten om viruset inte förhindras eller åtgärdas.

Övriga tjänsteföretag

Kitron Development:

R2 svarade att virus är vanligt förekommande men har hittills inte påverkat systemet på något sätt.

R2 menar på att om det skulle förekomma något virus är de snabba med att åtgärda detta virus. Eftersom det finns personal som är IT-kunniga menar R2 på att bra koll hålls på systemet vid virus och andra hot och risker som kan förekomma. R1 nämnde även att virus förekommer mest genom användning av e-post.

Generellt sett ser R1 på virus som ofta och vanligt förekommande vid användning av Internet.

Kapsch TrafficCom AB:

R4 svarade att virus förekommer men har inte drabbat systemet på något sätt.

R4 berättade att verksamheten har externa leverantörer som driftar och sköter verksamhetens säkerhet. Det finns mycket som stoppas med hjälp av de skyddsåtgärder som används från att drabba systemet förklarade R4.

Risken att system drabbas av virus generellt är stor om ingen säker säkerhetsåtgärd används menade R4. Generellt sett trodde R4 att virus är ett hot som troligen drabbar flera företag.

SYSteam:

R5 svarade att virus förekommer dagligen och berättade även att verksamheten drabbades av virus för två år sedan. R5 berättade att detta berodde på att verksamheten inte hade någon uttalad policy om antivirusskydd. Efter denna incidenten har policyn ändrats och virusskydd används flitigt berättade R5.

Generellt sett trodde R5 att virus är det största hotet som innebär en stor risk för ett företags system.

- Hacker

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar:

R1 svarade att ingen hacker har tagit sig igenom systemet. R1 menar på att det inte så tänkbart att någon skulle vilja hacka sig in i Länsförsäkringarnas system för rolighetens skull.

Generellt sett ser R1 detta hot som att det säkert förekommer inom olika verksamheter. R1 talade om att hackers är ett reellt hot som förekommit hos Ericsson, Telia m.fl. vilket det stått om i tidningar under åren.

SEB:

R3 svarade att ingen hacker har tagit sig igenom systemet på något sätt.

Vidare svarade R3 att hotet självklart finns och har säkert förekommer förekommit genom att de ”*knackat på dörren*” någon gång, men har inte lyckats ta sig in i systemet. R3 påpekade också att en hacker i sig inte är ett hot utan det är vad dessa gör som angripare i systemet som är de olika hoten.

Generellt sett såg R3 detta hot som ett hot som säkert förekommer men sedan om dessa lyckas ta sig igenom det som dessa är ute efter är svårt att säga.

Övriga tjänsteföretag

Kitron Development:

R2 svarade att verksamheten inte drabbats av att någon hacker försökt förstöra eller komma in i systemet.

R2 svarade vidare att någon hacker inte förekommit i verksamheten och ansåg att denna verksamhet förmodligen inte är något intressant för en hacker.

Utifrån vad som stått i tidningar under åren menade R2 att hackers *generellt* sett är vanligt förekommande vid andra typer av branscher som exempelvis Ericsson, Telia m.fl.

Kapsch TrafficCom AB: R4 kunde inte uttala sig om hur förekomsten av att hackers försöker hacka sig in i systemet ser ut eftersom företagets externa leverantörer sköter det arbete.

Däremot svarade R4 att verksamhetens system inte drabbats av något som en hacker varit ansvarig för. Verksamheten använder sig utav avancerade brandväggar som ständigt uppdateras som förhindrar utomstående att göra intrång i systemet.

SYSteam: R5 svarade att det är vanligt förekommande av hackningsförsök.

Alla hackningsförsök registreras genom loggning svarade R5. R5 berättade att verksamhetens system drabbats av ett hackningsförsök då en demosida blev ändrad. Hackningsförsöket kunde spåras med hjälp av loggning och de ansvariga polisanmäldes.

Generellt sett trodde R5 att hackningsförsöken förekommer hos många företag. R5 trodde också på att detta hot inte kommer bli mindre med tanke på att fler människor kommer få en bredare IT-kunskap samtidigt som systemen blir allt mer komplexare som kan ses som en utmaning för många.

- Obehörig åtkomst genom att skaffa användaridentitet och lösenord

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 svarade att detta hot aldrig förekommit i verksamheten. R1 menade på att det inte är vanligt att detta hot uppstår genom att personer utanför verksamheten skaffar användaridentitet och lösenord utan skulle vara mer vanligt att personer inom verksamheten står för detta hot.

R1 förklarar också att verksamheten har en säkerhetspolicy som talar om hur lösenord ska hanteras och användas av användarna för att ingen obehörig åtkomst ska förekomma genom att någon använder någon annans användaridentitet och lösenord. R1 svarade vidare att verksamheten använder sig utav enskilda lösenord och att inga grupplösenord används.

Generellt sett tror R1 att detta är ett hot som säkerligen förekommer inom olika verksamheter och att hotet i såfall förekommer via företagsspridning.

SEB: R3 svarade att hotet inte drabbat verksamheten men att det absolut är ett hot. R3 menade på att detta kan vara ett sätt för hackarna att jobba genom att knäcka lösenord. För att minska risken för detta hot används engångslösenord svarade R3.

Övriga tjänsteföretag

Kitron Development: R2 svarade att hotet inte har förekommit inom verksamheten och menade på att det skulle vara svårt för en utomstående person att komma åt användaridentitet och lösenord innanför verksamheten.

Om det *generellt* sett skulle förekomma skulle det isåfall ske genom att utomstående personer som städpersonal, vaktmästare som har tillgång till olika lokaler i verksamheten kommer åt en användaridentitet och lösenord. Detta är inget som förekommit i verksamheten konstaterade R2. R2 ansåg att om risken finns så uppstår detta hotet utifrån ett mänskligt fel innanför verksamheten.

Generellt sett anser R2 att detta hot kan vara vanligt förekommande internt än vad det är externt.

Kapsch TrafficCom AB: R4 svarade att hotet inte har drabbat företaget på något sätt.

Vid extern åtkomst till systemet använder verksamheten sig utav engångslösenord som kan likna det lösenordssystemet banker använder sig utav.

Generellt sett trodde R4 att risken är stor att en utomstående person kommer åt en anställds lösenord, med tanke på att många företag använder sig utav statiska lösenord som skrivs ner på papper och som lätt kan tappas bort och hamna i orätta händer.

SYSteam: R5 svarade att hotet inte förekommit inom verksamheten och därav inte drabbat systemet på något sätt. R5 svarade vidare

att verksamheten har en hög säkerhetspolicy för lösenordshantering.

Generellt sett trodde R5 att hotet är vanligt förekommande med tanke på att alla företag inte har en bra säkerhetspolicy av lösenordshantering.

- Åtkomst av känslig information i form av modifiering, tillägg eller borttagning av information.

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar:

R1 svarade att hotet inte har drabbat verksamheten men ser detta som ett reellt hot som kan påverka systemet och verksamheten stort.

R1 menar på att detta är ett stort hot mot Länsförsäkringar Bank då ekonomin, post eller bankgirot kan komma till stor skada. R1 förklarade också att det är förbjudet att användarna inom verksamheten kopplar upp sig mot Internet utanför Local Area Network (LAN) eftersom hot och risker lättare kan drabba systemet eftersom inga säkerhetsåtgärder finns som kan åtgärda möjliga hot som kan förekomma.

Generellt sett ser R1 detta hot som säkert förekommer lite överallt. R1 menar även här att hotet säkerligen drabbar vissa verksamheter mer än andra. Det är förmodligen inte lika intressant för en utomstående att ta sig in i vilken verksamhet som helst nämnde R1.

SEB:

R3 svarade här att hotet inte har drabbat verksamheten men ser det som ett absolut hot mot verksamheten.

Generellt sett trodde R3 att många företag förmodligen utsätts för detta hot. R3 förklarade att många företag som handhar viktig information som är intressant för den utomstående är dem som förmodligen drabbas mest av denna typ av hot. R3 menade på att eftersom SEB arbetar mycket med pengar kan verksamheten vara ett intressant val för den utomstående angriparen.

Övriga tjänsteföretag

Kitron Development: R2 svarade att hotet inte har förekommit i verksamheten. Generellt sett ser R2 detta hot som mer förekommande i andra branscher som verkar vara mer intressanta för den utomstående personen.

Kapsch TrafficCom AB: R4 svarade att hotet inte har förekommit i verksamheten på något sätt.

Generellt sett trodde R4 att hotet säkerligen är mer vanligt förekommande hos företag som arbetar med pengar, med tanke på att en utomstående person kan tänkas finna större intresse där pengar är inblandade.

SYSteam: R5 svarade att hotet inte drabbat verksamheten på något sätt. R5 svarade vidare, för att komma åt verksamhetens system måste man ha lösenord samt att all inloggning till systemet registreras genom loggning. På detta sättet blir det svårt för en utomstående att ta sig in i systemet och **om** hotet någon gång skulle förekomma kan en spårning göras med hjälp av loggningen.

- Åtkomst av känslig information i form av modifiering, tillägg eller borttagning av information.

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 svarade att hotet inte har drabbat verksamheten på något sätt men påpekade att detta är ett stort hot i Länsförsäkringar liksom i alla tjänsteföretag.

R1 menade på att viktiga filer och program ständigt lagras och skickas. R1 förklarade vidare att de ständigt skickar betalningar elektroniskt till både leverantörer som kunder varje dag där det rör sig om stora summor pengar.

Eftersom det handlar om ett samarbete som bygger på förtroende mellan Länsförsäkringen Bank och kunden är det viktigt att det inte uppstår hot som förstörande av filer och program samt åtkomst av känslig information som nämnts tidigare. R1 svarade också att användning av kryptering är relativt viktigt vid överföring av filer m.m.

Generellt sätt anser R1 detta hot som säkert förekommer men även här spelar det roll vilken bransch man talar om. Företag som arbetar mycket med pengar kan ses som en bransch som intresserar utomstående personer att snoka i.

SEB: R3 svarade på denna fråga detta hot inte har förekommit vad gäller förstörande av filer och program men sa även att allt kan hända. R3 svarade vidare att säkra skyddsåtgärder används för att förhindra denna typ av hot.

Övriga tjänsteföretag

Kitron Development: R2 svarade att hotet inte drabbat verksamheten då ingen utomstående person har rört verksamhetens filer eller program.

Kapsch TrafficCom AB: R4 svarade att verksamheten inte varit med om att verksamheten drabbats av detta hot.

R4 svarade vidare att förstörande av filer och program generellt sett är mer vanligt förekommande internt inom verksamheten än att externa personer står för detta hot.

SYSteam: R5 svarade hotet inte har förekommit eller drabbat verksamheten någon gång.

- Ändra innehåll på webbsidor

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 svarade att verksamhetens egen webbsida inte har drabbats av detta hot. R1 svarade vidare att hotet säkert förekommer.

SEB: R3 svarade att verksamheten har olika webbplatser där verksamheten själva ansvarar för en hemsida medan den andra hemsidan ansvaras av någon annan som konstruerat hemsidan.

Generellt sett såg R2 detta som ett stort hot som säkert förekommer vid de flesta webbsidor. Detta kan som nämnts tidigare exempelvis göras av hackers.

Övriga tjänsteföretag

Kitron Development: R2 svarade att hotet inte förekommit eller drabbat verksamhetens webbsida någon gång. Däremot trodde R2 att hotet generellt kan vara vanlig då det finns hackers som vill gå in på webbsidor för rolighetens eller politiskt syfte.

Kapsch TrafficCom AB: R4 svarade att hotet inte förekommit eller drabbat verksamhetens egna webbsidor men trodde att det är vanligt förekommande att webbplatser förstörs av exempelvis hackers och att fler och fler branschers webbservrar kommer att drabbas med tiden.

SYSteam: R5 svarade att detta hot är vanligt och de har haft ett intrång där en demowebbsajt blev ändrad. (se punkten om hackers). Händelsen blev dock spårad och polisanmäld.

- Risk för avlyssning av meddelande (trafik)

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 svarade att detta är ett riktigt hot mot verksamheten. R1 svarade vidare att hotet inte har förekommit i verksamheten.

R1 menade på att hotet inte kommer från hackarna eftersom dessa oftast jobbar för att ha kul. Detta är istället någon person som avlyssnar trafiken och det finns någon typ av uppsåt i botten som har med pengar att göra, då informationen är viktig för personen.

Generellt sett trodde R1 att hotet kan vara vanligt förekommande i speciella företag där informationen kan ses som viktig för den utomstående personen.

SEB: R3 svarade att hotet inte förekommit i verksamheten, inte vad de vet i varje fall. R3 svarade vidare att det är svårt att säga om hotet generellt är vanligt eller inte. R3 menade på att eftersom det finns så mycket trafik i systemet kan det vara svårt att avlyssna allt och därmed svårt för de utomstående att lyckas med att genomföra processen.

Övriga tjänsteföretag

Kitron Development: R2 svarade att hotet inte har förekommit i verksamheten.

Generellt sett trodde R2 att hotet kan förekomma beroende på vilken bransch det talas om. Vid branscher med pengar i bilden samt viktig information, finns det nog en större risk för avlyssning av trafik i systemet menade R2. R2 svarade vidare också att hotet kan tänkas förekomma mer vid trådlösa nät då det är lättare att avlyssna trafiken i systemet.

Kapsch TrafficCom AB: R4 svarade avlyssning av trafik inte har förkommit eller drabbat verksamheten någon gång. R4 svarade vidare att verksamheten har en uttalad policy om att känslig information som skickas via e-post måste krypteras och därav elimeneras risken för att någon obehörig person kommer åt informationen.

SYSteam: R5 svarade att verksamheten själva inte varit utsatta för detta hot men ser hotet är stort. R5 menade på att det inte är så svårt för en utomstående person att avlyssna trafik speciellt om bärbara datorer används.

- *Vad anser Ni vara det största externa hotet mot Ert IT-system med tanke på anslutning till Internet?*

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 svarade att alla hot som diskuterats är ett stort hot mot verksamheten. R1 menade på att verksamheten som alla andra tjänsteföretag arbetar mycket på förtroende med sina kunder och därmed är det oerhört viktigt att hoten inte drabbar företagen. Det är kostsamt att skydda sig mot hot och risker och ju mer företag vill skydda sig med 100% säkerhet desto dyrare för företaget blir det men måste dock göras förklarade R1.

SEB: R3 svarade att de största hoten mot IT-systemet är obehörig åtkomst vid känslig information då det är viktigt att känslig information inte hamnar i orätta händer. Andra hotet som R3 ansåg vara bland de största är virus som kan sänka systemets tillgänglighet och leda till väntetider med mera.

Övriga tjänsteföretag

Kitron Development: R2 svarade att hackers är ett av de största hoten då de kan göra intrång i systemet och förstöra filer eller ta över servrar

Kapsch TrafficCom AB: R4 svarade att det största hotet måste vara att IT-systemet drabbas av virus eller obehörig åtkomst i de interna servrarna.

SYSteam: R5 svarade att det största hotet mot IT-systemet är virus som finns av olika varianter. Om systemet exempelvis skulle utsättas för en trojan som är så aktiva kan allt kan hända väldigt fort.

D. Skyddsåtgärder verksamheten valt att använda

- *Vilka tekniska skyddsåtgärder anser Ni vara vanliga/nödvändiga bland **kryptering, behörighetskontrollsystem, brandvägg** och **antivirusprogram** för att åtgärda möjliga hot som kan drabba Ert företag vid en anslutning till Internet? Vid användning av nämnda skyddsåtgärder kan **fråga a** ställas och om inget användande av respektive skyddsåtgärd används ställs **fråga b**.*

  a) Varför används just denna skyddsåtgärd och till vilket syfte?
  b) Varför har Ni valt att inte använda Er utav denna skyddsåtgärd?

- *Kryptering*

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 svarade att kryptering används i stor utsträckning inom verksamheten. R1 svarade vidare att kryptering används för att hemlighålla viktig information så att den inte hamnar i orätta händer.

Alla betalningar som finns i systemet samt de betalningar som skickas via e-post krypteras alltid svarade R1. Kryptering är mycket nödvändigt eftersom verksamheten handhar känslig information som inte får hamna i obehörigas händer.

SEB: R3 svarade först att alla skyddsåtgärder som används är nödvändiga på sina egna sätt då de skyddar och uppfyller olika funktioner i systemet. Kryptering är därför som alla andra skyddsåtgärder en mycket nödvändig skyddsåtgärd

som används i syfte att skydda känslig information vid exempelvis e-post skickande svarade R3.

Övriga tjänsteföretag

Kitron Development: R2 svarade att kryptering är mycket nödvändigt att använda sig utav speciellt vid e-post skickande. R1 svarade vidare att den policy verksamheten har säger att alla bärbara datorer ska vara krypterade av den anledning att en utomstående person lätt kan stjäla en bärbar dator om den skulle glömmas bort någonstans. Kryptering används i syfte att hålla känslig information hemlig från obehöriga personer menade R2.

Kapsch TrafficCom AB: R4 svarade att kryptering ingår i VPN (Virtual Private Network) tekniken som används vid extern kommunikation. Kryptering används i övrigt vid e-postskickande av filer till syfte att skydda känslig information fr8n obehöriga personer.

SYSteam: R5 svarade att kryptering används vid mailtrafik och vid all annan information som anses vara känslig för företaget. Kryptering används i syfte till att skydda affärshemlig information.

- ***Behörighetskontrollsystem***

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: Denna skyddsåtgärd är absolut mycket nödvändig att använda för att åstadkomma säkerhet i IT-systemet svarade R1. R1 förklarade att det är viktigt att se varje anställds åtkomst i systemet så att varje rätt person har tillgång till rätt program.

R1 svarade vidare att loggning används till bland annat för att kunna läsa av en anställds åtkomst i IT-systemet. Vid gällande av lösenord förklarade R1 att inga grupplösenord används eftersom varje anställd ska ses som en enskild individ. Skulle det vara så att något oväntat händer i systemet blir det lättare att spåra vem det är som kan ligga bakom handlingen.

Syftet med behörighetskontrollsystemet är att kunna sätta behörigheter till de anställda så att de inte har access till alla

resurser i IT-systemet svarade R1. R1 menade på att rätt person ska ha använda rätt program vid rätt tidpunkt.

SEB:

R3 svarade att behörighetskontrollsystemet är en mycket nödvändig skyddsåtgärd som används i *syfte* att dela ut behörighet av systemets resurser till de anställda, och därmed se till att rätt person har tillgång till de rätta resurserna.

R3 berättade att verksamheten använder sig utav engångslösenord, på detta sättet blir det säkrare genom att ingen kan komma åt någon annans lösenordet eftersom den ständigt ändras.

Övriga tjänsteföretag

Kitron Development:

R2 svarade att behörighetskontrollsystemet är en mycket nödvändig skyddsåtgärd som används i verksamheten.

Syftet med användningen av denna skyddsåtgärd är att kunna sätta rätt behörighet till resurser till rätt person svarade R2. R2 förklarade även att om något skulle gå snett i systemet går det med hjälp av behörighetskontrollsystemet titta på vem som ansvarar för handlingen.

R2 svarade vidare att verksamhetens anställda tilldelats enskilda lösenord för att logga in till systemet. Vid detta sätt går det att se varje anställd som en enskild individ.

Kapsch TrafficCom AB:

R4 svarade att behörighetskontrollssystemet är som de andra skyddsåtgärder som används mycket nödvändig att använda sig utav.

R4 svarade vidare att verksamhetens anställdas enskilda lösenord byts ut vart tredje månad. För att komma åt systemet externt används SecureID doser som liknar bankers lösenordssystem svarade R4. R4 förklarade vidare att eftersom lösenorden ständigt byts ut minskar risken för att någon annan kommer åt lösenordet.

SYSteam:

R5 svarade att en mycket nödvändig skyddsåtgärd som används i stort sett för att se till att rätt person har tillgång till rätt resurser.

Vid intrång och attacker till systemet kan man med hjälp av behörighetskontrollsystemet göra en spårning. R5 berättade vidare att lösenord behövs för att logga in till systemet och att ingen kan logga in sig som anonym, detta för säkerhetens skull.

- ***Brandvägg***

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar:

R1 svarade att brandvägg är en mycket nödvändig skyddsåtgärd som används flitigt. På grund av att verksamheten samarbetar med 24 andra länsförsäkringsbolag används avancerade brandväggar där *syftet* är att skydda det privata nätverket från andra nätverk, samt att kontrollera och begränsa trafiken till systemet.

R1 berättade även att verksamheten köper up2date från andra som ser till att brandväggen alltid är uppdaterad och rätt konfigurerad. R1 menade på att det skulle bli väldigt kostsamt för verksamheten om någon utomstående skulle komma förbi brandväggen eftersom verksamheten jobbar med tjänster som bygger på förtroende, därför är det viktigt att satsa på avancerade brandväggar som uppehålls av experter.

SEB:

R3 svarade att brandväggen som alla andra nämnda skyddsåtgärder är en mycket nödvändig skyddsåtgärd som används.

Syftet med brandväggen är att den ska kontrollera att rätt trafik kommer in i systemet.

Övriga tjänsteföretag

Kitron Development:

R2 svarade att brandväggen är en absolut nödvändig skyddsåtgärd.

R2 svarade vidare att *syftet* med användning av brandväggen är att spärra portar för att kontrollera trafiken som kommer in eller ut i systemet. Eftersom det är viktigt att rätt trafik kommer in i systemet använder verksamheten sig utav avancerade brandväggar som ständigt uppdateras.

Kapsch TrafficCom AB: R4 svarade att brandväggen är en absolut nödvändig skyddsåtgärd som måste användas med tanke på hur mycket trafik som kan komma utifrån. R4 menade på att denna trafik måste kontrolleras så att endast rätt trafik till systemet tas emot.

R4 svarade vidare att brandväggen uppdateras kontinuerligt till nya versioner för att upprätthålla säkerheten. R4 påpekade att det är de externa leverantörerna som nämnts tidigare som står för denna grundsäkerhet.

SYSteam: R5 svarade att ett antal brandväggar används i verksamheten och att dessa är mycket nödvändiga för säkerheten.

R5 svarade vidare att brandväggar används i syfte att låsa systemet hårt så att ingen onödig trafik kommer in, när rätt trafik kommer in i systemet öppnas de portar som behövs som sedan låses igen.

- ***Antivirusprogram***

Tjänsteföretag som arbetar med elektroniska penningstransaktioner

Länsförsäkringar: R1 svarade att antivirusprogram är en mycket nödvändig skyddsåtgärd som används till syftet att förhindra virus från att påverka systemet. Antivirusprogram är viktig att uppdatera ständigt samt att antivirusprogrammet är rätt konfigurerat.

SEB: R3 svarade att antivirusprogram är mycket nödvändig att använda sig utav i syfte att skydda systemet mot virus och förhindra virus från att sprida sig i systemet.

Övriga tjänsteföretag

Kitron Development: R2 svarade att antivirusprogram är mycket nödvändigt att använda sig utav i *syfte* att förhindra virus som kan sprida sig i systemet. R2 svarade vidare att verksamheten använder en av de säkraste antivirusprogram som finns för att förhindra virus från att drabba systemet på något sätt.

Kapsch TrafficCom AB:

R4 svarade att antivirusprogram används flitigt i verksamheten och är absolut nödvändig att använda sig utav i *syfte* att förhindra virus att sprida sig i systemet. R4 berättade vidare att antivirusprogram används på olika nivåer som exempelvis clienter, servrar olika protokoll (smtp, http m.fl.).

R4 berättade också att uppdateringen av antivirusprogrammen sker en gång i timmen. Uppdateringen av antivirusprogram är väldigt viktig för att fånga majoriteten av de virus som kan förekomma påpekade R4.

SYSteam:

R5 svarade att antivirusprogram är en mycket nödvändig skyddsåtgärd som måste användas i syfte att stoppas virus från att sprida sig i systemet. R5 svarade vidare att antivirusprogrammen används på filnivå i servrar, clienter och i mail. De antivirusprogram som används kan avlyssna, förhindra, reparera och ta bort virus påpekade R5.

7 Analys

I detta kapitel kommer först en analys redovisas utifrån resultatet i materialpresentationskapitlet och den problemställning som ligger till grund för detta arbete.

7.1 Utvärdering och analys av insamlat material

Detta arbete har som syfte att ta reda på om de hot som anses vara vanliga i samband med en anslutning till Internet enligt litteraturen (se kapitel 2) är vanligt förekommande hos olika verksamheterna i studien samt om nämnda skyddsåtgärder i litteraturen (se kapitel 2) anses vara nödvändiga hos olika verksamheter. Utifrån denna problemprecisering kan paralleller till den urvalsgrupp som valet för undersökningen göras. Urvalsgruppen består av fem olika verksamheter där samtliga har en central IT-enhet som behandlar IT-frågor. Två av de utvalda verksamheterna är av branschen tjänsteföretag som arbetar med elektroniska penningstransaktioner och de andra tre verksamheterna är av branschen övriga tjänsteföretag. Valet att ta med två olika branscher som tjänsteföretag och tillverkandeföretag var för att undersöka huruvida det finns några skillnader av förekomsten av hotbild samt om skyddsåtgärderna anses vara lika nödvändiga i båda branscherna. Eftersom alla verksamheterna i studien har en anslutning till Internet samt att verksamheterna arbetar med IT-säkerhet exempelvis genom att ha en uttalad policy för att skydda sig mot olika hot så anses verksamheterna ha goda kunskaper om hur hotbilden ser ut och vad man bör göra för att åtgärda hoten. Verksamheterna som ingått i studien anses ha haft en hög relevans för arbetets problemställning. Det låga antalet respondenter som ingick i studien kan dock ses som en nackdel och kan bidra till att det kan vara svårt att dra några slutsatser av resultatet i studien.

För att hitta lämpliga respondenter för de olika verksamheterna, har som tidigare nämnts kontakt tagits via telefon till verksamheternas IT-säkerhetsansvariga. I den första kontakten presenterade jag mig och förklarade lite kort om studiens syfte. I stort sett alla IT-säkerhetsansvariga ansåg sig själva vara mest insatta i området och därför lämpliga respondenter. Alla medverkande respondenter har varit medverkande eller har kunskap om verksamhetens IT-säkerhet och det kan därför konstateras att respondenterna har varit representativa för undersökningen. Alla respondenter har varit väldigt tillmötesgående under intervjuerna och den enda som kan ses som nackdelen under dessa intervjuer är att några av respondenterna haft mycket mer åsikter och tankar att berätta om ämnet än de andra och att svaren för varje fråga därför blivit lite varierande bland respondenterna.

Det insamlade materialet från intervjuerna anses ha en bra validitet eftersom de frågor i intervjulaget som ställts har gett den information som avsågs att få fram i undersökningen. Något som dock höjer validiteten är att de flesta respondenterna som intervjuats har mångårig praktisk erfarenhet av IT-säkerhetsarbete och således besitter goda kunskaper inom området.

Med tanke på arbetets problemställning har de frågor som ställts varit relevanta då de gav de svar som bidrar till ett resultat av studien. De flesta svar blev tillräckligt långa och detaljrika. Eftersom en bandspelare valdes att användas vid nästan alla intervjuerna för att spela in svaren upplevdes det som tryggare om alla svar inte kunde antecknas fullt. För att ytterligare minimera risken för feltolkningar frågades det om möjlighet att skicka resultatet via e-post till respondenterna så de kunde läsa igenom svaren och redigera texten om det skulle behövas.

7.2 Analys av resultatet

De verksamheter som återfinns i resultatet har haft fokus på olika verksamhetsområden vilket har varit intressant då hotbilden vid anslutning till Internet kan se annorlunda hos olika branscher samt att de olika skyddsåtgärderna (se kapitel 2) kan anses vara mer eller mindre nödvändiga hos olika verksamheter. I denna undersökning ingår verksamheter från branscherna tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag. I samtliga verksamheter anses det extremt viktigt att ha en uttalad policy för hur hot som kan förekomma vid anslutning till Internet ska åtgärdas.

7.2.1 Analys av intervjufrågorna

Utifrån ett antal grundläggande frågor har en lösning till problemställningen sökts. En sammanställning och analys av intervjusvaren från de olika verksamheterna redogörs nedan.

A. Analys av respondenternas tidigare erfarenheter och dennes trovärdighet inför denna undersökning.

- *Vad är din befattning och hur många år har du arbetat inom detta område?*

Samtliga respondenter säger sig ha någon form av utbildning inom området IT. Några av respondenterna har även kunskaper och erfarenheter inom området IT-säkerhet vad gäller externa hot vid anslutning till Internet samt kunskap om skyddsåtgärder för att åtgärda hoten vilket har fåtts genom arbetserfarenhet. Två av fem respondenter (R3 och R5) arbetar som IT-säkerhetsansvariga, de andra två respondenterna R1 och R4 arbetar som IT-ansvariga och R2 som systemadministratör.

Det finns ingen större skillnad mellan respondenternas arbetspositioner, då alla har ett jobb som innefattar arbete inom området IT-säkerhet. R5 och R3 arbetar som IT-säkerhetsansvariga och kan av denna anledning anses ha en djupare kunskap inom område då de ansvarar för IT-säkerheten inom verksamheten. De övriga respondenterna som har en position som IT-ansvarig/systemadministratör har en stor kunskap inom området men inte lika stor som IT-säkerhetsansvariga då de själva inte ansvarar för hela IT-säkerhetsarbetet. Detta tyder på att samtliga har tillräckligt mycket kunskap inom området IT-säkerhet och passar därav urvalskriterierna för att vara med denna undersökning.

R1 har arbetat åtta år i sin position som IT-ansvarig, vilket är en betydligt längre period än vad de övriga respondenterna har arbetat. Detta kan beror på att R1 är äldre än de övriga

respondenterna, men eftersom åldern inte har varit ett faktum för urvalskriterierna inför undersökningen har detta ingen betydelse för resultatet.

B. Analys av verksamhetens användning av Internet och syn på risker med Internetanslutning

- *Ge en kort beskrivning av vad företaget använder Internet till?*

Samtliga respondenter ansåg att Internet används som ett praktiskt redskap för att utföra de vardagliga arbetsuppgifterna som exempelvis informationssökning. Vidare används Internet för e-post och för att hålla kontakt med omvärlden. Användning av Internet varierar lite mellan de olika verksamheterna då de har olika sysselsättningar men syftet med att ha en anslutning till Internet är för verksamheterna enhetlig. Några verksamheter använder också Internet för att ladda ner olika program vid exempelvis uppdatering av virusprogram och brandvägg. De som inte laddar ner uppdateringsprogram från Internet köper istället dessa tjänster från externa leverantörer.

I materialet kan man se att användningsområdena kommunikation med e-post, informationssökning samt affärer på Internet används i ungefär lika stor utsträckning hos alla verksamheter. Dessa användningsområden används av nästan alla verksamheter och drar därför slutsatsen att dessa användningsområden är de viktigaste bland svenska företag och kasnke den främsta anledningen till att de ansluter sig till Internet. Skillnaden ligger dock i att verksamheterna har olika sysselsättningar och därmed skiljer sig användandet av Internet från verksamhet till verksamhet. All denna användning utav Internet tyder på att verksamheterna är fullt medvetna om vad Internet har att erbjuda och ser därför Internet som ett praktiskt hjälpmedel för att utföra sina vardagliga uppgifter.

- *Har Ni en fast anslutning till Internet?*

Den anslutning som verksamheterna använder sig utav har för alla intervjuade verksamheter varit en fast anslutning. En sammanfattande analys av denna fråga utifrån resultatet är att verksamheternas fasta anslutning bidrar till att IT-systemet kan utsättas för fler hot då systemet alltid är kopplad till Internet. Det positiva med en fast anslutning antas vara att Internets tjänster alltid finns tillgängliga samt att denna typ av uppkoppling lönar sig ekonomiskt för verksamheterna.

- *Ser Ni några risker med att företaget är anslutet till Internet? Varför?*

Respondenternas svar var relativt entydiga. Samtliga verksamheter i intervjuerna anser att det finns en självklar hotbild och risk med att vara ansluten till Internet. Vid en anslutning till Internet ser verksamheterna detta som en risk då vägar öppnas för utomstående att skada verksamhetens system som kan sänka systemets effektivitet. Detta tyder på att verksamheterna är. Verksamheterna är starkt medvetna om risken som finns och arbetar starkt för att förebygga hoten och riskerna med hjälp av skyddsåtgärder och genom att ha en uttalad policy för IT-säkerheten.

Detta tyder på att alla verksamheterna i denna undersökning har tillräckligt med kunskap om vilken säkerhetsrisk det finns i samband med en uppkoppling mot Internet. Det finns en tendens att tro att verksamheternas syn på den risk som finns i samband med en anslutning till Internet varierar då tjänsteföretagen antagligen upplever en större risk med Internet med tanke på att de arbetar mycket med pengar.

C. Analys av verksamhetens externa hotbild vid anslutning till Internet.

- *Vilken extern hotbild anser Ni vara vanliga i förhållande till Ert IT-system vid anslutning till Internet vad gäller:*

- ***Virus***

Samtliga verksamheterna ser virus som ett hot som förekommer vardagligen. Av de intervjuade verksamheterna har endast en av dem drabbats av virus, orsaken var att verksamheten inte hade någon uttalad policy för virusskydd. Idag har verksamheten som de andra intervjuade verksamheterna en väl uttalad policy för virusskydd och ingen har drabbats av virus på något sätt. E-post är där virus förekommer mest svarade de flesta respondenterna. Generellt ser verksamheterna virus som ett stort hot om inte det största som förekommer och som troligen drabbar företag som inte förhindrar eller åtgärdar viruset med hjälp av skyddsåtgärd.

Någon större skillnad finns dock inte hur tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag upplever virus. Detta kan bero på att virus är ett hot som kan drabba vilket system som helst oavsett branschtyp. Däremot kan virus tänkas upplevas som ett större hot hos tjänsteföretag som arbetar med elektroniska penningstransaktioner med tanke på att viktig data som behandlar pengar kan gå förlorad och som kan leda till att kunder tappar förtroendet för dessa tjänsteföretag. Det kan av denna anledning antas vara så att tjänsteföretagen väljer att satsa mer på att förebygga detta hot från att drabba systemet genom avancerade antivirusprogram. Att bara en av verksamheterna drabbats av virus kan bero på att de övriga verksamheterna från början haft tillräcklig kunskap för att veta hur de ska skydda sig mot virus.

- ***Hackers***

Av de intervjuade verksamheterna ansåg R3 och R5 hackningsförsök som vanligt förekommande genom att de försöker ”knacka på dörren”. Respondenten R5 berättade att verksamhetens system en gång drabbats av ett hackningsförsök då en demosida blev ändrad, som tur gav detta inga negativa effekter för verksamheten då det var en testsida de hade hackat sig in i. De övriga respondenterna har inte varit med om att någon hacker försökt förstöra eller komma in i systemet. Respondent R4 kunde inte uttala sig om hur vanligt det är att hackningsförsök förekommer vilket är rimligt då det är de externa leverantörerna som sköter säkerhetshanteringen, men påpekade att verksamhetens system inte har drabbats av någon hacker någon gång. R3 tyckte att en hacker i sig inte kan ses som ett hot utan istället som en angripare, det är de skador angriparen orsakar som är de olika hoten. Generellt sett ser verksamheterna detta hot som troligen vanligt förekommer och drabbar företag.

Det finns dock en skillnad på hur tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag upplever hot från hackers. Övriga tjänsteföretag ser hackers som ett absolut hot mot systemet men anser sig själva inte som utsatta. Detta kan bero på att företag där pengar är inblandade är de mest utsatta med tanke på att dessa företag troligen är mer intressantare för den utomstående. Att tjänsteföretag som arbetar med elektroniska penningstransaktioner känner sig mer utsatta för detta hot kan bero på att de är medvetna om att det de arbetar med kan tänkas vara intressant för en utomstående att komma åt.

- ***Obehörig åtkomst genom att skaffa användaridentitet och lösenord***

Samtliga respondenter svarade att obehörig åtkomst till systemet genom att en utomstående skaffat sig ett användaridentitet och lösenord inte har förekommit i verksamheterna och därav inte drabbat någon av dem. Många av respondenterna anser att detta är ett hot som är mer förekommande intern inom verksamheten än vad det gör extern. Respondenten R5 ansåg generellt att detta hot troligen kan vara vanligt förekommande externt med tanke på att alla företag inte har en uttalad policy vad gäller lösenordshantering. Respondenten R3 ansåg också att hotet kan ses som vanligt förekommande generellt med tanke på att många företag använder sig utav statiska lösenord som inte byts ut så ofta, dessa lösenord skrivs ner på lappar och kan lätt tappas bort och hamna i obehörigas händer. Generellt sett ser större delen av respondenterna detta hot som troligen förekommer bland företag men att risken ser större ut internt än externt. För att minimera risken att någon utomstående ska kunna logga in sig på någon annans lösenord används inga grupplösenord utan enskilda lösenord används för varje anställd. Några av verksamheterna använder sig utav engångslösenord som anses vara det säkraste sättet för att eliminerar risken för att hotet ska inträffa. Vad gäller lösenord är det viktigt att verksamheten har en väl uttalad policy för lösenordshantering ansåg respondenterna.

Svaren från denna fråga har varit mycket enhetlig då svaren inte skiljer sig åt så mycket. En tolkning av svaren är att obehörig åtkomst genom att skaffa användaridentitet och lösenord

anses vara mer vanligt internt än externt och upplevs därför inte som ett större hot. Att bara ett företag i denna undersökning anser detta hotet vara lika förekommande externt som intern kan tolkas som att företaget har en djupare kunkap om hur vanligt förekommande detta hotet är externt. En reflektion över svaren från denna fråga är att det är viktigt att verksamheterna själva inser att möjligheten att hotet kan förekomma externt som internt.

- ***Åtkomst av känslig information i form av modifiering, tillägg eller borttagning av information.***

Samtliga respondenter säger att verksamheterna inte har drabbats av denna typ av hot någon gång. Då säkra skyddsåtgärder används inom verksamheterna blir det svårt för den utomstående att ta sig in i systemen. Respondenternas svar var relativt entydiga om att denna typ av hot är mer förekommande hos branscher där det finns något intressant att hämta för den utomstående, det kan exempelvis handla om branscher som arbetar mycket med pengar. Respondenterna R1 och R3 som är av branschen tjänsteföretag ser detta som ett allvarligt hot som kan innebära negativa effekter och stor skada för verksamheten. Detta kan ses som rimligt då tjänsteföretag som arbetar med elektroniska penningstransaktioner som exempelvis bankers arbete bygger på samarbete och förtroende med sina kunder. Generellt sett förekommer troligen hotet lite överallt men att det finns vissa branscher som är mer utsatta än andra.

Svaren från verksamheterna visar en stor skillnad mellan hur tjänsteföretag och tillverkande företag upplever hotet. Det går att se att tjänsteföretag som arbetar med elektroniska penningstransaktioner ser sig själva som mer utsatta för åtkomst av känslig information i form av modifiering, tillägg eller borttagning av information än andra branscher. Övriga tjänsteföretag ser inte sig själva som utsatta utan säger att andra branchtyper som tjänsteföretag kan tänkas vara mer drabbade av detta hot. En tolkning utifrån detta resonemang är att tjänsteföretag som arbetar med elektroniska penningstransaktioner som övriga tjänste företag är fullt medvetna om att detta hot oftast förekommer hos tjänsteföretag då den utomstående finner mer intresse att komma åt den information som tjänsteföretag behandlar. Det finns också en tendens att tro att tjänsteföretag som arbetar med elektroniska penningstransaktioner vid ett sådant här hot har mycket mer att förlora än övriga tjänsteföretag.

- ***Förstörande av filer och program***

På denna fråga svarade samtliga respondenter att hotet inte anses ha förekommit eller drabbat verksamheterna. Respondenterna är här relativt entydiga om att säkra skyddsåtgärder bör användas för att minimera risken för att ett hot som denna ska förekomma och i värsta fall drabba verksamheten negativt. Hotet kan ses som mycket allvarlig speciellt hos tjänsteföretag som ständigt lagrar filer och som ständigt skickar betalningar elektronisk till både kunder och leverantörer varje dag där det rör sig om stora summor pengar. Respondenterna anser som tidigare hot att förekomsten av hotet beror lite

på vilken bransch man talar om. Generellt sett är detta ett hot som enligt respondenterna troligen förekommer lite överallt men som drabbar vissa branscher mer än andra.

Den stora skillnaden mellan mellan de två branscherna tros bero på att stora summor pengar ständigt lagras och skickas i filer och därav upplevs detta hot som allvarligare hos tjänsteföretag som arbetar med elektroniska penningstransaktioner.

- ***Ändra innehåll på webbsidor***

Av alla verksamheterna som varit med i intervjuundersökningen har endast en drabbats av att någon utomstående har ändrat innehållet på en webbsida. Hackers är den angriparen som anses vara ett stort hot för denna typ av skada. Respondenterna ansåg att hotet generellt sett säkerligen förekommer och att det till stor del genomförs av hacker som gör detta för rolighetens och politiskt syfte.

Någon större skillnad finns inte mellan hur tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag upplever detta hot. Detta kan tänkas bero på att ändring av innehåll på webbsidor kan drabba vilken webbsida som hels oavsett branschtyp. Det finns en tendens att hackers möjligen har försökt knackat på verksamheteternas dörrar men att de inte lyckats ta sig igenom p.g.a. säkra skyddsåtgärder verksamheterna använder sig utav. Att bara en verksamhet har drabbats utav detta hot kan antingen bero på att hackarna har varit så pass kunniga och har på så sätta tagit sig igenom, eller så kan det bero på att skyddsåtgärderna inte varit tillräckligt säkra för hackningsförsök

- ***Risk för avlyssning av meddelande (trafik)***

Avlyssning av trafik av någon utomstående har inte drabbat någon av verksamheterna någon gång. Respondenterna anser även vid detta hot att det beror lite på vilken bransch man talar om. Den person som avlyssnar trafik har säkert något uppsåt i botten som exempelvis har med pengar att göra. Samtliga respondenter ansåg också att det är viktigt att kryptera all känslig information och på detta vis elimineras risken för att någon utomstående kan avlyssna trafiken. Några av respondenterna påpekade att risken för avlyssning av trafik är mycket större vid användning av bärbara datorer.

Materialet visar att det finns en stor skillnad mellan hur tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag upplever hotet. Den stora skillnaden visar att tjänsteföretag som arbetar med elektroniska penningstransaktioner anses vara mer utsatt för risk för avlyssning av trafik, vilket kanske inte är så förvånande eftersom denna typ av bransch handhar sådan information som kan vara av intresse för den utomstående samt att pengar finns inblandade.

- *Vad anser Ni vara det största externa hotet mot Ert IT-system med tanke på anslutning till Internet?*

Majoriteten säger att virus och obehörig åtkomst är bland de största externa hot som kan drabba IT-systemet. Det kan anses som självklart då känslig information kan hamna i orätta händer vid obehörig åtkomst samt att virus i hög grad kan sänka IT-systemets tillgänglighet och effektiviteten. R1 anser dock att alla hot kan ses som lika stora då skada av IT-systemet kan uppstå genom alla hoten.

Det verkar finnas en tendens att större delen av verksamheterna ser virus och obehörig åtkomst som de största hoten. En anledning till varför just dessa hot anses som de största kan vara att hoten är så pass farliga att de kan drabba och förstöra systemet som kan i sin tur påverkar hela verksamhetens sysselsättning.

D. Skyddsåtgärder verksamheten valt att använda

- *Vilka tekniska skyddsåtgärder används bland **kryptering, behörighetskontrollsystem, brandvägg** och **antivirusprogram** för att åtgärda möjliga hot som kan drabba Ert företag vid en anslutning till Internet? Vid användning av nämnda skyddsåtgärder kan **fråga a** ställas och om inget användande av respektive skyddsåtgärd används ställs **fråga b**.*

c) *Varför används just denna skyddsåtgärd och till vilket syfte?*
d) *Varför har Ni valt att inte använda Er utav denna skyddsåtgärd?*

- ***Kryptering***

Syftet med verksamheternas användning av kryptering ar att skydda känslig affärsinformation så att den inte kan läsa av någon obehörig person som inte har behörighet till informationen. Vidare används kryptering for att säkerställa mailtrafiken och den externa kommunikationen. Detta kan anses vara självklart då verksamheterna ständigt skickar och tar emot känslig information från exempelvis leverantörer eller kunder. Verksamheterna anser att kryptering är en mycket nödvändig skyddsåtgärd som bör användas for att skydda all känslig information från att hamna i obehörigas händer.

Krypteringens användning och till vilket syfte krypteringen används är lika för att verksamheter tjänsteföretag som tillverkandeföretag. Kryptering kan dock ses som viktigare och lite mer av absolut måste hos tjänsteföretag som arbetar med elektroniska penningstransaktioner eftersom de ständigt skickar och tar emot filer som innehåller känslig information samt stora summor pengar. Av denna anledning prioriteras kryptering mycket högt. En reflektion över syftena med att använda kryptering ar att det ar viktigt att verksamheterna själva inser hur viktig informationen är för dem och krypterar den därefter sa att den inte bara krypteras for att följa regler.

- ***Behörighetskontrollsystem***

Samtliga verksamheter anser att denna typ av skyddsåtgärd är mycket nödvändig att använda sig utav i syfte att se varje anställds åtkomst i systemet så att rätt person har tillgång till rätt program. Det är ingen av verksamheterna som använder sig utav grupplösenord, detta kan vara tänkas vara uppenbart då varje anställds ska ses som enskilda individer. Två verksamheter (R4 och R3) nämnde att de använder sig utav engångslösenord för att vara på den säkra sidan. Dock använder verksamheten endast engångslösenord vid extern åtkomst av systemet sa R4. För övrigt använder samtliga verksamheter sig utav enskilda lösenord. Det kan på detta sätt tänkas bli enklare att se varje anställds åtkomst i systemet. Om problem uppstår i systemet exempelvis av en attack eller att någonting helt enkelt går snett till kan BKS ses som ett mycket bra hjälpmedel för att spåra den som ansvarar för handlingen anses verksamheterna. Verksamheterna ser BKS som en mycket nödvändig skyddsåtgärd och som ett bra hjälpmedel vid krissituationer.

BKS och dess tre funktioners (lösenord, åtkomstkontroll & loggning) syften skiljer sig någorlunda mellan verksamheterna. Att ingen av verksamheterna använder sig utav grupplösenord tenderas bero på att det anses vara riskabelt då fler personer kan komma åt lösenordet samt att varje anställd ska kunna ses som enskilda individer. Om något skulle gå snett i systemet kan det tänkas vara enklare att spåra den person som orsakat skadan om enskilda lösenord används. Att bara två verksamheter använder sig utav engångslösenord vid extern åtkomst av systemet kan tänkas bero på att de satsar på en säker inloggning där ingen annan på något sätt kan komma åt varandras lösenord.

- ***Brandvägg***

På denna fråga har de samtliga intervjuade svarat att trafiken till och från systemet måste kontrolleras så att endast rätt trafik kommer in i systemet. Det verkar vara rimligt med tanke på den mängd trafik som kan komma utifrån. Av detta syfte är brandväggen ett säkert och mycket nödvändigt val för verksamheterna. Samtliga verksamheter är väl medvetna om att brandväggar måste uppdateras till den senaste versionen för att erhålla säkerheten. Några av de intervjuade påpekade även att de använder sig utav avancerade brandväggar som inte går att ladda ner från nätet utan som måste köpas. Detta val har gjorts för att hålla IT-systemet extra säkert från omvärlden.

Utifrån materialet kan ingen större skillnad av användning utav brandvägg mellan verksamheterna diskuteras. Att några av verksamheterna valt att använda sig utav avancerade brandväggar kan tänkas bero på att säkerheten ska vara den högsta och därmed minskar också risken för intrång och onödig trafik

- ***Antivirusprogram***

Enligt de intervjuade är virus ett av de största hoten som kan drabba deras IT-system. Med tanke på detta svarade samtliga verksamheter att antivirusprogram absolut måste användas i

syfte att förhindra virus att sprida och föröka sig i systemet. Även denna skyddsåtgärd uppdateras av samtliga verksamheter och ser till att antivirusprogrammet är rätt konfigurerat. Några av de intervjuade svarade på denna fråga som på ovanstående frågan att de väljer att köpa avancerade program för att erhålla det bästa skyddet mot virus.

Eftersom virus anses vara bland de största hoten mot IT-systemet är det uppenbart varför verksamheterna väljer att satsa på en högre säkerhet som avancerade antivirusprogram. Detta tyder på att verksamheterna har en djup kunskap om hur och vilka skyddsåtgärder som finns att tillgå och för att skydda sig mot de olika hoten.

8 Slutsats

Den slutsats som framkommit genom resultatet med utgångspunkt från arbetets problemställning är att den hotbild som presenterats i kapitel 2 utifrån litteraturstudier stämmer överens med hur verksamheten upplever hotbilden. Några av hoten har förekommit inom verksamheterna, någon enstaka har även drabbats av enstaka hot. Oavsett om verksamheterna blivit drabbade av hoten eller inte ser de hoten som självklara hot som förekommer och kan drabba verksamheterna om de inte skyddar sitt system med säkerhetsåtgärder. Tjänsteföretagen som arbetar med elektroniska penningstransaktioner i denna undersökning upplever dock några av hoten som allvarligare i jämförelse till de övriga tjänsteföretagen. Detta kan bero på att tjänsteföretagen som arbetar med elektroniska penningstransaktioner kan ta större skada och förlora oehört mer än övriga tjänsteföretag med tanke på att dem arbetar med pengar och arbetar med ett stort förtroende till sina kunder.

Denna undersökning har genomförts inom olika verksamheter där sysselsättningen skiljer sig åt. Trots det begränsade urvalet av respondenter kan resultatet anses som en fingervisning om hur verksamheterna ser på den hotbild som finns i samband med en anslutning till Internet samt hur skyddsåtgärderna används. Utifrån resultatet kan en slutsats dras att hotbilden skiljer sig åt mellan branscherna tjänsteföretag som arbetar med elektroniska penningstransaktioner och övriga tjänsteföretag. Många av de hot som presenterats i kapitel 2 betraktas vara allt mer allvarligare, större och anses drabba företag av branschen tjänsteföretag som arbetar med elektroniska penningstransaktioner mer än övriga tjänsteföretag.

Utifrån resultatet kan slutsatsen om de skyddsåtgärder som presenterats i kapitel två dras att verksamheterna anser samtliga skyddsåtgärder vara mycket nödvändiga att använda för att åtgärda hoten. Skillnaderna mellan verksamheternas hotbild vid en anslutning till Internet visar ingen större skillnad på hur de olika skyddsåtgärderna används. Kryptering är den skyddsåtgärd som har en större viktighet hos tjänsteföretagen som arbetar med elektroniska penningstransaktioner än övriga tjänsteföretag. Eftersom hoten obehörig åtkomst, förstörande av filer och program och avlyssning av trafik är ett så stort hot hos tjänsteföretag som arbetar med elektroniska penningstransaktioner är det mycket tänkbart

att kryptering är en skyddsåtgärd som prioriteras väldigt högt för att åstadkomma ett säkert IT-system.

Att inte verksamheterna i denna undersökning drabbats eller att hot inte ens förekommer kan med goda skäl bero på att de är så pass säkerhetsmedvetna och använder skyddsåtgärder som hindrar dessa hot från att drabba systemet. Huvudsyftet med att använda varje skyddsåtgärd har varit samma för alla verksamheter.

9 Diskussion

I detta kapitel följer diskussioner över resultat, genomförandet och erfarenheter under arbetsprocessen. Avslutningsvis ges förslag på fortsatta arbeten.

9.1 Diskussion angående resultatet av undersökningen

Syftet med detta arbete har varit att få en inblick i vilka hot som anses vara vanligt förekommande hos verksamheter som använder sig utav Internet till sitt vardagliga arbete samt kunna se om hotbilden skiljer sig åt mellan olika branscher. Uppsatsens syfte har också varit att undersöka om användning av skyddsåtgärder bland verksamheterna påverkas utifrån den hotbild som finns samt hur nödvändiga skyddsåtgärderna som tagits fram ur litteraturundersökningen är bland olika verksamheter.

Det resultat som tagits fram kan inte ses som generella eftersom intervjustudien enbart omfattar 5 respondenter. Tanken var att studien skulle omfatta ett större antal deltagande respondenter men på grund av olika faktorer var detta inte möjligt.

Även om resultatet endast omfattar ett fåtal verksamheter så anses slutsatsen kunna gälla även en större undersökning. Valet av verksamheter tros inte ha påverkat slutsatsen på ett missvisande sätt då det redan vid ett fåtal intervjuer visats att förekomsten av de olika hoten skiljer sig åt mellan verksamheterna. En undersökning omfattande fler verksamheter tros ge liknande slutsats dock kanske det skulle gå att se ett tydligare mönster för hur hotbilden skiljer sig åt bland de olika verksamheterna som skulle klassas efter olika branscher. Hotbilden kommer troligtvis att öka med tanke på att allt fler börjar bli IT-kunniga samt att systemen kommer att bli allt komplexare. Detta komplexa system kan innebära en utmaning för många av de IT-kunniga. Skyddsåtgärderna kommer troligtvis att utvecklas och avanceras allt mer efter hoten. För övrigt har resultatet stämt bra överens med det förväntade resultatet.

Resultatet kan ses som tillförlitligt eftersom besöksintervjuer och telefonintervjuer genomförts och att respondenterna tagit sig tid att besvara frågorna utförligt. Respondenterna har enligt mitt tycke besvarat de ställda frågorna ärligt och jag ser därför inte någon anledning att misstro svaren eftersom det inte ställts några känsliga frågor. Det har varit fritt fram för respondenterna att berätta mer än vad som frågats efter och detta har resulterat i att vissa har berättat mer än andra. Det som verksamheterna har berättat utöver de ställda frågorna har tagits med då detta ansetts vara intressant.

9.2 Erfarenheter

De erfarenheter som erhållits under detta arbetes gång är bland annat när examensarbetet påbörjades verkade tiden vara väl tilltagen men tiden har sprungit iväg och en lärdom som erhållits är att allt tar mer tid i anspråk än vad som kan förmodas. Litteraturstudierna för detta examensarbete har varit väldigt omfattande. Det har varit svårt att finna material som varit direkt knutet till syftet för rapporten. Först tog processen att söka material längre tid än förväntat och därefter vidtog inläsningsfasen på problemområdet.. att dela upp faser och avsnitt för att lämna in har upplevts som positivt.

Det visade sig att det var svårt att till en början få respondenter till undersökningen men det ordnade sig i sista minuten och fem stycken intervjuer blev genomförda. Vetskapen om att de flesta har ont om tid gör att man blir väldigt tacksam till dem som verkligen tar sig tid att dela med sig av sina erfarenheter. Intervjutiden blev något utdragen men genomfördes i bestämd tid. Att intervjua upplevdes som positivt då respondenterna var välvilliga och hjälpsamma., vilket gjorde att intervjuerna blev relativt lyckade.

9.3 Förslag till fortsatt arbete

Nedan följer ett antal frågeställningar som uppkommit under arbetet med detta examensarbete och som kan vara intressanta att undersöka. Det finns med största sannolikhet många fler problem att undersöka inom området IT-säkerhet.

- Det kan vara intressant att i en ny undersökning försöka kartlägga de interna hot som kan förekomma inom verksamheter, samt kartlägga vad verksamheterna gör för att minska risken för dessa hot (ex. Utbildning, säkerhetspolicy).

- Ytterligare ett förslag till fortsatt arbete är att undersöka om säkerhetspolicyn och utbildning om säkerhet som ges inom verksamheten är någon nytta för de anställda. Detta för att se om utbildning och säkerhetspolicyn kan ses som ett hjälpmedel för de anställda. Denna undersökning kan exempelvis genomföras genom intervjuer.

Referenser

Ahlberg, J (1998) *Jonas Webresurs*, Tillgänglig på Internet www.jonasweb.nu/datorn/hackers.html [Hämtat 2003-11-12]

Ahuja, V. (1996) *Network and Internet security,* Boston : AP Professional. ISBN 0-12-045595-1

Andersson, M. Carlsson, T. & Åkerman, S. (1996) *Nyckeln till World Wide Web* : version 1.0. Stockholm : Norstedt. ISBN 91-1-953261-X

Bell, J. (1995) *Introduktion till forskningsmetodik (2: a upplagan)*. Lund: Studentlitteratur

Borg, T. Lozano, A. Löfgren, T. Malmgren, S. Palicki, J. (1997) *IT-säkerhet för ditt företag*. Uddevalla: Bonnier Datamedia. ISBN 91-644-0196-0

Dawson, C. W. (1999) The Essence of Computing Projects: A Student´s Guide. Prentice Hall: Huvudlitteratur. ISBN 0-13-021972-X

Fors, A. (2003) *Internet för nybörjare*, Tillgänglig på Internet www.home.swipnet.se/afors/_private/internet1.htm [Hämtat 2003-10-20]

IFI (2003) IT *Hantering av IT-incidenter - Åtgärder mot dataintrång och skydd av IT-system.* Tillgänglig på Internet www.inst.ifi.se/program-incident.htm [Hämtat 2003-11-02]

Kommunikationsdepartementet "Riktlinjer för uppdrag till Statskontoret", bilaga till regeringsbeslut nr. 11, Internet, (http://194.251.183.23:81/itsaker.htm), [Hämtat 031115]

Lantz, A. (1993) *Intervjumetodik: den professionellt genomförda intervjun,* Lund: Studentlitteratur. ISBN 91-44-38131-X

Lindberg, B. (1993) *Client/server och säkerhet.* Stockholm : DF (Dataföreningen i Sverige). ISBN 91-86656-68-6

Nordstedts ordbok AB (1999) *Nya svenska ordboken*. Göteborgs universitet: Språkdata och Nordstedts Ordbok. ISBN 91-7227-109-4

Patel, R & Davidson, B (1994) Forskningsmetodikens grunder, att planera, genomföra och rapportera en undersökning (Andra upplagan). Lund: Studentlitteratur. ISBN 91-44-30952-X

SIG Security (1998) *Säkerhetsarkitekturer,* Lund: Studentlitteratur. ISBN 91-630-7263-7

Statskontoret (1998a) *Handbok i IT-säkerhet Del 1-Introduktion.* Stockholm: CM Gruppen AB. ISBN 91-7220-288-2

Statskontoret (1998b) *Handbok i IT-säkerhet Del II-Policy, ansvar och organisation.,* Stockholm: CM Gruppen AB. ISBN 91-7220-288-X

Statskontoret (1998c) *Handbok i IT-säkerhet Del III-Skyddsåtgärder,* Stockholm: CM Gruppen AB. ISBN 91-7220-288-X

Sårbarhets- och säkerhetsutredningen (2001) *Säkerhet i en ny tid*. , Stockholm: Statens Offentliga Utredningar. ISBN 91-38-21462-8

Vacca, J. (1996). *Virtual reality: strategies for Intranet and World Wide Web applications*. (Första upplagan).Charleston : Computer Technology Research Corp. ISBN 1-56607-971-3

Vxu, (2003) *Säkerheten och samhället,* Tillgänglig på Internet www.masda.vxu.se/multimedia/km/security/security.htm#Shot [Hämtat 2003-10-13]

WebWay AB (2002), WebWay – Professionella Internettjänster, Tillgänglig på Internet www.webway.se/certs/intro/nycklar.shtml [Hämtat 2003-10-14]

Wedberg, H (1997) ” Uppdatera säkerhetsrutinerna annars blir det dyrt” och ” Organisera IT-säkerhetsarbetet”, IT-nyheterna nr7, sid 10

Bilaga 1

Information om kommande intervju

”Rapportens rubrik är externa hot och skyddsåtgärder vid anslutning till Internet”.

Examensarbetets frågeställning lyder:

- *Vilken hotbild är vanlig i förhållande till Ert IT-system vid anslutning till Internet vad gäller nedanstående hot? Har nedanstående hot någon gång förkommit eller drabbat Ert IT-system? Hur tror Ni att hotbilden ser ut generellt?*

    - ***Virus***
    - ***Hackers***
    - ***Obehörig åtkomst genom att skaffa användaridentitet och lösenord***
    - ***Åtkomst av känslig information i form av modifiering, tillägg eller borttagning av information.***
    - ***Ändring av innehåll på webbsidor***
    - ***Avlyssning av meddelanden inom företaget***

Om något av de ovanstående hot är vanliga, varför tror Ni detta hot förekommer?

- *Vilka av de nedanstående nämnda tekniska skyddsåtgärder använder Ni för att åtgärda externa hot vid anslutning till Internet och i så fall till vilket syfte?*

    - ***Kryptering***
    - ***Behörighetskontrollsystem***
    - ***Brandvägg***
    - ***Antivirusprogram***

Det är de ovanstående nämnda externa hot och skyddsåtgärder som kommer att tas upp vid intervjun. Denna avgränsning har valts att göra på grund av att IT-säkerhet är ett så omfattande område.

Tack på förhand!

Med vänlig hälsning
Rakhi

Bilaga 2

Intervjufrågor

Nedan redovisas intervjufrågorna

11. Vad är ditt namn och vad är din befattning?

12. Hur många år har du arbetat på företaget?

13. Ge en kort beskrivning av vad företaget använder Internet till.

14. Har ni en fast anslutning till Internet?

15. Ser Ni några risker med att företaget är anslutet till Internet? Varför?

16. Vilken hotbild anser Ni vara vanliga i förhållande till Ert IT-system vid anslutning till Internet vad gäller nedanstående hot? Har nedanstående hot någon gång förkommit eller drabbat Ert IT-system? Hur tror Ni att hotbilden ser ut generellt?

    g) Virus
    h) Hackers
    i) Obehörig åtkomst genom att skaffa användaridentitet och lösenord
    j) Åtkomst av känslig information i form av modifiering, tillägg eller borttagning av information.
    k) Förstörande av filer och program
    l) Ändra innehåll på webbsidor
    m) Risk för avlyssning av meddelanden inom företaget

17. Vad anser Ni vara det största externa hotet mot Ert IT-system med tanke på anslutning till Internet?

18. Vilka tekniska skyddsåtgärder används bland ***kryptering, behörighetskontrollsystem, brandvägg och antivirusprogram*** för att åtgärda möjliga hot som kan drabba Ert företag vid anslutning till Internet? Vid användning av nämnda skyddsåtgärder kan fråga 8a ställas och om inget användande av respektive skyddsåtgärd används ställs fråga 8b.

    c) Varför används just denna skyddsåtgärd och till vilket syfte?
    d) Varför har Ni valt att inte använda Er utav denna skyddsåtgärd?

19. Övriga frågor?