Kandidatuppsats, 10 poäng i informatik

IT-relaterade hot

- professionella IT-tjänstemäns farhågor och möjligheter

Framlagd: 09-12-2005

Författare: Marcus Holmquist
Oscar Stibeck

Handledare: Anders Svensson

Abstract

The objective of this thesis was firstly to examine the possibilities of creating a universal tool for evaluating IT-security. When all the material was gathered we saw that we had strayed away from our subject and that our focus was on IT-threats and IT-professionals apprehensions and possibilities on the subject. The purpose of this thesis was there after to find and identify threats and counter measures in publications and later discuss these with IT-professionals. We found and identified several threats that the professionals encountered in their work. These threats ranged from techniques used by hackers to threats that can arise when the users on the network are poorly educated. The counter measures that were identified were firstly the usual well-known ones such as firewalls, intrusion detection systems and antivirus programs. Later on in our research we found other counter measures such as PAPAI and SBA Scenario that are overall solutions for preventing a network from being violated. When we had had our discussions with the IT-professionals we could tell that some threats occur more frequently than others and that some counter measures were more suitable than others.

Key words: IT-security, IT-threats, hackers, preventive measures

Nyckelord: IT-säkerhet, IT-hot, hackers, förebyggande lösningar

Innehållsförteckning

Abstract 2
Innehållsförteckning 3
Figurer 5
1 Inledning 6
1.1 Bakgrund 6
1.2 Problemformulering 6
1.3 Syfte 7
1.4 Preliminära avgränsningar 7
1.5 Målgrupp 7
1.6 Disposition av uppsatsen 7
2 Metod 9
2.1 Val av litteratur 10
2.2 Datainsamling 10
2.2.1 Primärdata 10
2.2.2 Sekundärdata 11
2.3 Val av elektroniska källor 11
2.4 Intervjuer 11
2.5 Reliabilitet och validitet 12
2.6 Källkritik 12
3 Begreppteori 14
3.1 Informationssäkerhet 14
3.2 Olyckor och misstag 16
3.3 Insiderproblem 17
3.4 Underleverantörer och outsourcing 17
3.5 Hotskala 18
3.6 Hackermetoder 19
3.7 Malicious Software 21
3.7.1 Virus 21
3.7.2 Spionprogram 21
3.7.3 Keyloggers 22
3.7.4 Trojanska hästar 22
3.7.5 Worms (Maskar) 22
3.8 Brister inom applikationer 22
3.9 Åtgärder mot IT-hot 23
3.9.1 Firewalls 23
3.9.2 IP security (IPsec) 23
3.9.3 Kryptering 24
3.9.4 Intrusion detection 25
3.10 Verktyg för att förebygga brister inom IT-säkerhet 27
3.10.1 ISO-standarden 17799 27
3.10.2 SBA Check 28
3.10.3 SBA Scenario 28
3.10.4 PAPAI 28
3.10.5 Proactive Network Security 35

4 Intervjuer 37
4.1 Intervju med Magnus Persson, LDC 37
4.2 Intervju med Björn Ivarsson, SecureIT 39
4.3 Intervju med Johan Westlind, TeliaSonera/Portal 40
5 Analys och diskussion 42
5.1 Hot som berör omedvetenhet 42
5.2 Riktade attacker 43
5.3 Mjuk- och hårdvara för att skydda sig mot IT-hot 44
5.4 Verktyg för att arbeta i förbyggande syfte mot IT-hot 45
6 Slutsatser 47
7 Källförteckning 49
7.1 Publicerade källor 49
7.2 Muntliga källor 50
7.3 Elektroniska källor 50

Figurer

Figur 3.1 – IT-säkerhet, SIS

Figur 3.2 – IT-säkerhet, SIS

Figur 3.3 – Hotbild, SIS

Figur 3.4 – Hotskala, egen efter SIS

Figur 3.5 – Shared library attacks, Buchanan

Figur 3.6 – Packet sniffing, Buchanan

Figur 3.7 – Public-Key Cryptograpy, Stallings

Figur 3.10 – Översikt, Länk 6

Figur 3.11 – Verksamhet, Länk 6

Figur 3.12 – Omgivning, Länk 6

Figur 3.13 – Policy, Länk 6

Figur 3.14 – Analys, Länk 6

Figur 3.15 – Plan, Länk 6

Figur 3.16 – Arkitektur, Länk 6

Figur 3.17 – Implementering, Länk 6

1 Inledning

Inledningen har till syfte att ge en bakgrund till varför denna uppsats skrivs och vilka skäl författarna hade för uppsatsens problemformulering. Förutom bakgrund och problemformulering innehåller denna del även syfte samt preliminära avgränsningar.

1.1 *Bakgrund*

I dagens företagsklimat är IT-avdelningen en kritisk faktor för att verksamheten skall fungera. Information som finns inom företaget måste kunna skyddas. Det gäller företagshemligheter och den personsonliga integriteten hos alla anställda. Skydd mot datorintrång blir allt mer komplicerat då metoderna för att penetrera IT-system ständigt utvecklas. Företag är inte ensamma om behovet av en gedigen säkerhet. Flera organ inom samhället som till exempel militären, skatteverket, ams, kommuner, landsting med många fler är också starkt beroende av att IT-säkerheten är god. Bankkontor har på senare år valt att lägga mycket av sin verksamhet på Internet då man lägger ned kontor runt om i landet. Postorderfirmor har på samma sätt övergått till att lägga sin verksamhet på Internet. Då företag går över från den fysiska världen till Internet oavsett bransch kommer man vara tvungen att ha säkerhet som en viktig del i sin nya strategi.

1.2 *Problemformulering*

Vi kontaktade Anders Svensson som är kursansvarig för bland annat INF 369, Säkerhet i Nätverk och Databaser, för att få hjälp med förslag till ämne. Anders ville se en uppsats om att kartlägga tänkbara säkerhetsparametrar som man skulle kunna använda i ett mätverktyg. Efter att materialet var sammanställt och intervjuerna var gjorda märkte vi att vi hade drivet bort från vårt ursprungliga ämne och att en annan frågeställning passade vår uppsats bättre. Då vi hade lagt mycket fokus kring vad intervjuobjekten hade för åsikter kring IT-säkerhet kändes det naturligt att anpassa vår frågeställning efter detta.

Den slutgiltiga frågeställningen blev därefter:

IT-relaterade hot – professionella IT-tjänstemäns farhågor och möjligheter

IT-relaterade hot är ett mycket aktuellt ämne. Vi erfar att förståelsen kring dessa hot är samlade kring en liten grupp av människor inom IT-sektorn. Med denna frågeställning hoppas vi kunna dela med oss av vad IT-tjänstemän har för funderingar kring IT-hot och vilka åtgärder som lämpas i olika miljöer.

1.3 *Syfte*

Genom att undersöka problem och hinder som förekommer inom IT-relaterade hot och åtgärder avser vi att försöka undersöka vad profesionella IT-tjänstemän anser om dessa problem, samt hur de går till väga motverka dessa.

1.4 *Preliminära avgränsningar*

Vi har valt att begränsa denna studie till tre intervjuobjekt samt teoretiska studier. Alla intervjuobjekt är professionella aktörer inom IT-sektorn. Vi anser att mycket input från tre intervjuobjekt och nära samarbete med dem under uppsatsens gång gynnade oss mer än att ha fler personer som vi inte kan ägna lika mycket tid.
Beträffande teori har vi försökt ge en överskådlig granskning av ämnet och där det hör hemma har vi beskrivit teorin mer i detalj. Denna blandning bör leda till relevanta slutsatser.
Under intervjuerna som har gjorts i samband med uppsatsen har deltagarna delat med sig av yrkeshemligheter och sårbarheter inom IT-system, inte bara allmänt utan även sina egna. Av denna anledning har vi valt att inte transkribera de bandade intervjuerna utan sammanfattat det som vi tyckte var mest relevant i kapitel 4. Intervjudeltagarna har fått läsa igenom vår sammanfattning för att godkänna den innan uppsatsen slutfördes. Vi anser att detta medför en stärkt integritet för den information vi har blivit betrodda med.

1.5 *Målgrupp*

Denna uppsats är främst riktad mot studenter, forskare samt andra i ämnet väl insatta personer. Terminologin och språkvalet kan i vissa fall ses som avancerad och vissa stycken kräver att läsaren har en grundläggande förståelse av TCP/IP.

1.6 *Disposition av uppsatsen*

Vi har valt att skriva en kvalitativ rapport med lineär struktur, vilket innebär att den följer den logiska uppläggningen introduktion, problem (frågeställning), metod, analys och slutsatser. Till skillnad från den traditionella rapporten saknar den kvalitativa rapporten en direkt standard för utformning men vi kommer att börja med att behandla undersökningens syfte, motiv, fråga eller problem. Vi kommer sedan att gå vidare och visa vår använda metodik, där t.ex. miljöer, kontexter och processer som vi studerat kommer att skildras. Efter metodiken kommer erhållen information att presenteras för att i nästa skede sedan utvärderas. Avslutningsvis kommer en analys och slutsats. Det läsaren kan förväntas sig är ett teoretiskt berättande utifrån empiriskt material om de punkter som berör IT-säkerhet och sedan med hjälp av IT-experters analys och kommentarer förslag på vad som är väsentligt beträffande studiens ämne. Andra karaktäristika drag som är typiska för den kvalitativa rapporten är förutom valet av

disposition även bestämning av fokus, identifikation av målgrupp (läsekrets) samt revision. Valet av fokus hänger samman med undersökningens syfte och målgrupp. Vid revisionen ges de som berörts av studien en chans att granska rapporten. Dessa kommentarer och synpunkter kan ofta bidra till ändringar och tillägg som måste tas med i den slutgiltiga rapporten (Backman, 1998).

Kapitel 2, metoddelen, kommer att beskriva hur vi stötte på oväntade uppgifter som gjorde att vi fick tänka om och disponera om uppsatsen.

kapitel 3, begreppteorin, behandlar fakta som finns kring ämnet. Här presenteras olika sätt att beskriva IT-säkerhet och vilka aspekter som berör IT-säkerhet i form av hot och åtgärder.

Kapitel 4 går igenom det material och åsikter som intervjuobjekten hade.

Kapitel 5 består av en analys. Kapitel 3 och kapitel 4 lägger en grund för kapitel 5, som kommer baseras på innehållet i dessa kapitel. Här diskuteras både teorin och inputen från intervjuerna för att få fram vilka IT-hot som är mest väsentliga samt hur man kan förbereda sig mot dessa.

Kapitel 6 avslutar uppsatsen med slutsatser kring rapporten.

2 Metod

För att försäkra oss om god kvalitet av denna uppsats valde vi att gå igenom en checklista för olika punkter att tänka på innan man påbörjar ett forskningsprojekt. Denna checklista har bl.a. till syfte att bidra till en kvalitetsförbättring samt att kontrollera att ämnet verkligen är relevant. Checklistan ställer frågor såsom:

- Är det meningsfullt att forskningen äger rum?
- Låter det sig göras?
- Omfattar undersökningen rätt saker?
- Kommer undersökningen att ge sanningsenliga och ärliga resultat?
- Kommer undersökningen att resultera i en rättvisande och balanserad bild?
- Hur hanterar du de rättigheter och känslor som de involverade har?

Är det meningsfullt att forskningen äger rum?

I vår mening är det meningsfullt att undersöka vad experter ute på fältet har för åsikter kring vad som utvecklas inom deras verksamhet.

Låter det sig göras?

I vårt fall fanns det inga synliga förhinder till varför denna frågeställning skulle vara onormalt svår att genomföra. Teorin finns i både elektronisk och i tryckt form och det finns möten med IT-tjänstemän inplanerade.

Omfattar undersökningen rätt saker?

Denna checkpunkt är väldigt relevant för denna uppsats. Inledningsvis följde vi en annan frågeställning som hade för uppgift att finna säkerhetsparametrar för att mäta IT-säkerhet. När allt material var insamlat visade det sig att undersökningen inte omfattade rätt saker. Efter samtal med olika föreläsare på institutionen för informatik vid Lunds Universitet bestämde vi oss för den frågeställning som är gällande för uppsatsen. När denna omställning var gjord tycker vi att undersökningen nu verkligen omfattar rätt saker.

De återstående tre punkterna hoppas vi kunna säkerställa genom gedigen objektivitet.

2.1 *Val av litteratur*

Vid val av litteratur kan tre metoder av sökning göras: konsultation, manuell sökning samt datorbaserad sökning (Backman, 1998). I syfte att få en heltäckande bild av ämnet har vi använt oss av alla tre metoderna. Inledningsvis användes främst konsultation och manuell sökning för att få en överblick om ämnets omfång och en tidig indikation på vad som gjorts tidigare inom området. Konsultation skedde av bl. a. handledare som i ett tidigt skede kom med rekommendationer av användbara böcker. Angående den manuella sökningen valde vi att överskådligt granska den litteratur på Lunds Universitetsbibliotek som berör ämnet IT-säkerhet och därefter göra avgränsningar till vilken litteratur som skulle användas. Den litteratur som kom att ge störst vikt i den tekniska förklaringen i uppsatsen blev, William Buchanan, Mastering Networks, 1999. Att boken är tryckt 1999 skulle vanligtvis ses som ett hinder men i detta fall uppskattas det var en fördel eftersom det material och information som är tagen ur Mastering Networks ständigt återkommer i nutida nätverksböcker. Detta ser vi som en indikation på att det är korrekt och ännu relevant fakta. Böcker som används till stöd i den tekniska förklaringen är Network Security Essentials (Stallings, 2003) och Intrusion Detection (Gurley Bace, 2000). I öppningsskedet av denna uppsatsskrivning använde vi oss av SOU 2004:32 (Statens Offentliga Utredningar) för att få definitioner att bygga våra slutsatser på. SOU:s material känns högst pålitligt eftersom informationen därifrån kommer ett statligt organ och förhoppningsvis saknar egenintressen. Eftersom boken är skriven 2004 är informationen färsk och uppdaterad. Vetenskapliga tidskrifter som publicerats har hämtats från universitetsdatabaser och sådant som har funnits i eftertryck på Lunds Universitet. ELIN är ett exempel på databas som använts, där bl. a. artikeln ”Proactive Network Security: Making Your Network Unassailable” (Keanini, 2005) fanns. Detta är en nypublicerad artikel som är högst aktuell och var till nytta vid vår egen analys av IT-säkerhet. Användandet av kompletterande artiklar utöver böcker ses som en fördel då böcker ofta har en längre produktions- och distributionstid än artiklar som är skrivna samma år och därför gör dessa mer aktuella. Något som bör påpekas är dock att användandet av en enda referensdatabas inte alltid ses som tillräckligt eftersom de kanske inte alltid är heltäckande. Detta på grund av att en viss fördröjning finns innan helt ny litteratur hunnit komma med i databasen.

2.2 *Datainsamling*

Backman (1998) skiljer på primärdata och sekundärdata. Det är förtjänstfullt att använda sig av bådadera när man skriver en uppsats. Sekundärdatainsamling skiljer sig från primärdatainsamling på så vis att det handlar om att återanvända redan skaffade data.

2.2.1 Primärdata

Primärdata i vår studie består av intervjuer med tre olika anställda inom IT-branschen som har till syfte att skildra dessas åsikter om IT-säkerhet. Eftersom data från tidigare undersökningar inte finns tillgänglig blir primärdatans betydelse för uppsatsens kvalitet

av största vikt. Med hjälp av observationer i empirin skapar vi en kontakt med verkligheten och därmed en bättre förståelse. Vi valde intervjuobjekten eftersom deras arbetsuppgifter handlar om att analysera IT-hot.

2.2.2 Sekundärdata

Backman (1998) menar att det är viktigt att studera litteratur och undersökningar inom det valda problemområdet för att kunna lyckas med utförandet av sin undersökning. Lämpligt är enligt Backman att man tar del av tidigare studier som gjort inom området innan man påbörjar sin egna studie. Man bör också granska tidigare undersökningar samt deras resultat eftersom detta kan hjälpa en att lättare hitta fokus på det man egentligen vill undersöka.

2.3 *Val av elektroniska källor*

Stor del av denna forskning har gjorts med hjälp av källor på Internet. På grund av att informationen på Internet kan vara opålitlig har författarna valt att koncentrera sig till elektroniska källor som ligger under välkända domännamn, statliga organ, universitetsinstitutioner och erkänt pålitliga institut. Vi anser att dokumentation som ligger på ovannämnda siter har genomgått mer vetenskaplig granskning och kan således betraktas som pålitligare.

Med detta sagt vill författarna ta upp ett undantag gällande det som beskrivits om elektroniska källor. I ett stycke i kapitel 3.7 är en elektronisk källa tagen från Wikepedia. Det kan tyckas märligt att författarna har valt ett sådant uppslagsverk men just i detta fall är beskrivning utomordentligt bra för de ändamål kapitlet har. Dessutom återfinns just Wikepedias förklaring på ett antal större etablerade IT-säkershetssiter.

En elektronisk källa som bidragit enormt mycket till denna uppsats och varit till stor inspiration för författarna är www.papai.se (Policy, Analys, Plan, Arkitektur and Planning). Beskrivningar kring papai återfinns i kapitel 4.

2.4 *Intervjuer*

De tre intervjuobjekt vi har valt är Björn Ivarsson, Secure IT, Magnus Persson Datasäkerhetssamordnare LDC, Johan Westlind, Telia/Portal. Ivarsson och Persson har båda lång erfarenhet inom IT-branschen medan Johan Westlind har kortare och är relativt nyexaminerad Unixadministratör. Vi har valt denna blandning för att få olika synvinklar. Medan Ivarsson och Persson förlitar mycket av sin kunskap på yrkeserfarenhet och vidareutbildning bygger Westlinds värderingar på vad han lärde sig under sin aktuella utbildning och sin begränsade arbetstid i IT-miljö.

Björn Ivarsson arbetar som IT-konsult med arbetsuppgifter som inkluderar att evaluera datasäkerhet hos företag och utbildar personal vid implementering av säkerhetspolicies.

Magnus Persson har arbetet med IT i 23 år. Under denna tid har han arbetat som systemerare på Tetra Pak och Securitas. Sedan 1987 har han arbetat på Lunds universitet där han började programmera ekonomisystem. Persson har en ADB utbildning avslutad 1980.

Johan Westlind är utbildad Unixadministratör från Nackademin. Utbildningen avslutades 2005. Samtidigt som Westlind utbildades arbetade han hos Telia som Unixadministratör och under tiden denna uppsats skrevs bytte Westlind uppdragsgivare till Portal. Vi anser inte att detta skall medföra några hinder då intervjun redan var avslutad innan Westlind bytte arbetsgivare.

2.5 *Reliabilitet och validitet*

Bell och Robert (1992) anser följande om reliabilitet och validitet. Allt material som man använder sig av oavsett form måste granskas kritiskt för att, dels avgöra hur tillförlitlig (reliabel) samt hur giltig (valid) informationen som man fått fram är. Medan reliabilitet avser att man mäter på ett tillförlitligt sätt avser validitet det som är relevant i sammanhanget. För att försäkra oss om att god validitet har uppnåtts har vi noggrant studerat ämnet, IT-säkerhet, och fördjupat oss i terminologin i syfte att bättre kunna göra bedömningar huruvida materialet är giltigt eller inte. Vi har varit noggranna med att enbart göra inspelade eller loggade intervjuer med personer som har lång erfarenhet inom sitt yrke och väl insatta i de problem som IT-hot kan föra med sig. För att undvika eventuella missförstånd lät vi de intervjuade personerna ta del av det sammanställda intervjumaterialet i efterhand för att ge dem möjlighet att kommentera. Med hjälp av duglig kvalité på den tekniska utrustningen vi använde oss av för att logga intervjuerna samt bra kunskaper om hur dessa skulle utföras kunde vi säkerställa reliabiliteten, dvs. kontrollera att mätningen utfördes på ett tillförlitligt sätt. Vi ville även se till att i förväg försäkra oss om att de intervjuade personerna var väl förberedda på intervjuns uppbyggnad och val av ämne. Detta gjorde vi genom att skicka frågorna i god tid innan intervjutillfället så att de fick chans att läsa på och undvika eventuella överraskningar samt bättre kunna svara på frågorna.

2.6 *Källkritik*

Ändamålet med källkritik är att se till att källan är korrekt i sina antaganden och genom det ger den validitet. Av dessa anledningar har vi valt att helt utesluta populärvetenskapliga tidskrifter då sådana inte genomgår tillräcklig oberoende och sakkunnig, vetenskaplig granskning.

Alla ämnen som berör teknik och framförallt datorrelaterad information är under ständig utveckling och denna utveckling sker väldigt fort. Författarna tog hänsyn till detta och

använde sig material som är relativt uppdaterad för att försäkra sig om att de äldre referenserna fortfarande är pålitliga. Just detta har varit en grundsten i uppsatsen då författarna har använt sig av lite äldre referensmaterial i vissa stycken. Genom att nyttja metoden att använda gammal litteratur och jämföra den med ny hoppas författarna att uppsatsen tillhandahåller god validitet.

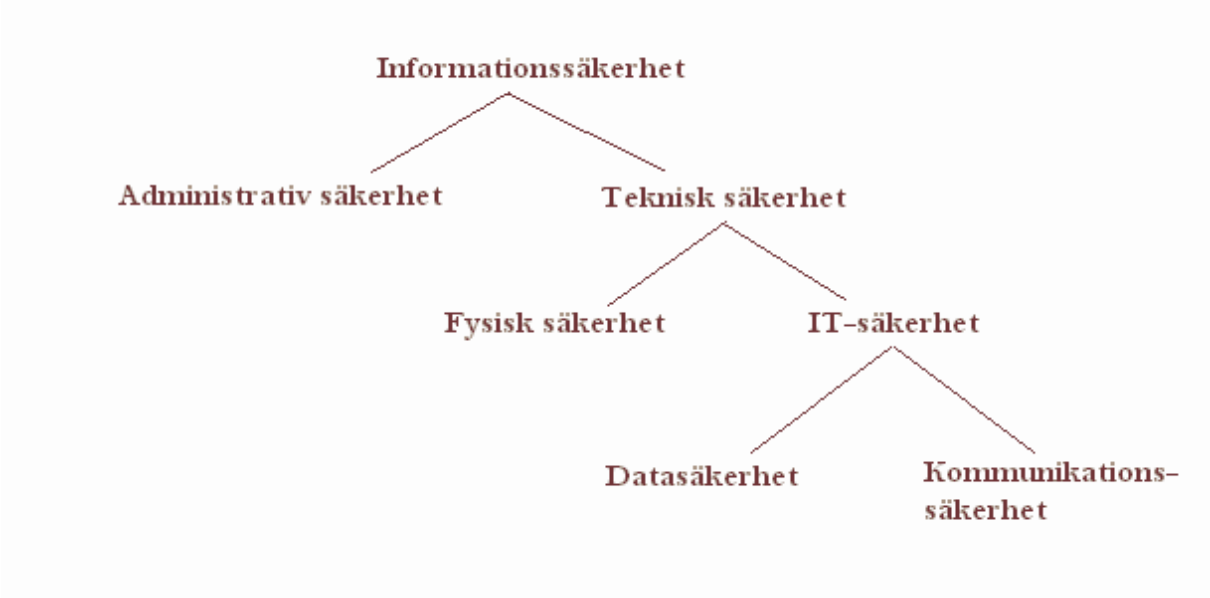
Kritisk granskning gäller alla källor, såväl de muntliga som de skriftliga. Det är av yttersta vikt att granska alla källor väl då detta är den viktigaste delen i urvalsmetoden. Först finna de källor man vill använda sig av, avgränsa sig till det som är av intresse i källan. Sedan jämföra denna källa med andra för att se om andra skribenter håller med. När det gäller muntliga källor har författarna valt att intervjua personer med lång erfarenhet i branschen som besitter positioner som kräver mycket god kunskap inom området IT-säkerhet för att överhuvudtaget kunna sköta sitt arbete. På så vis hoppas författarna ha försäkrat sig om att kompetensen hos de intervjuade är tillräcklig (Bell och Robert, 1992).

3 Begreppteori

Teorin i detta kapitel ligger till grund för att senare kunna dra slutsatser kring hot och möjligheter kring IT-relaterade hot. Inledningsvis skildras olika tolkningar av IT-säkerhet. Dessa skildringar kommer huvudsakligen från statens offentliga utredningar. Därefter övergår teorin till tekniska aspekter som rent konkret berör IT-säkerhet. Det handlar om olika metoder att komma över känslig data och även åtgärder för att skydda sig mot intrång. Till sist avslutas kapitlet med helhetstäckande lösningar för att skydda sin verksamhet mot IT-hot. Dessa består av en ISO standard, tre olika verktyg och ett säkerhetstänkande hämtat ur ”Proactive Network Security: Making Your Network Unassaible” av Tim Keanini.

3.1 *Informationssäkerhet*

Enligt SIS (SOU 2004:32), kan informationssäkerhet beskrivas på flera olika sätt, beroende på ändamål. Ett sätt är att utgå från skyddsåtgärdernas miljö, teknisk respektive administrativ säkerhet etc. Administrativ säkerhet omfattar bl. a. metoder, regelverk, organisation, utbildning och kontroll. Modellen nedan beskriver Informationssäkerhet ytligt enligt detta perspektiv:



Figur 3.1 – IT-säkerhet, SOU 2004:32

En annan vanlig uppdelning av begreppen som också nämns av SIS är följande modell:

Figur 3.2 – IT-säkerhet, SOU 2004:32

En av SIS (SOU 2004:32) definitioner av begreppet IT-säkerhet är:

”*...utredningen definierar informationssäkerhet som säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet samt spårbarhet och oavvislighet. Begreppet innefattar såväl IT-säkerhet som säkerhet i administrativa rutiner”.*

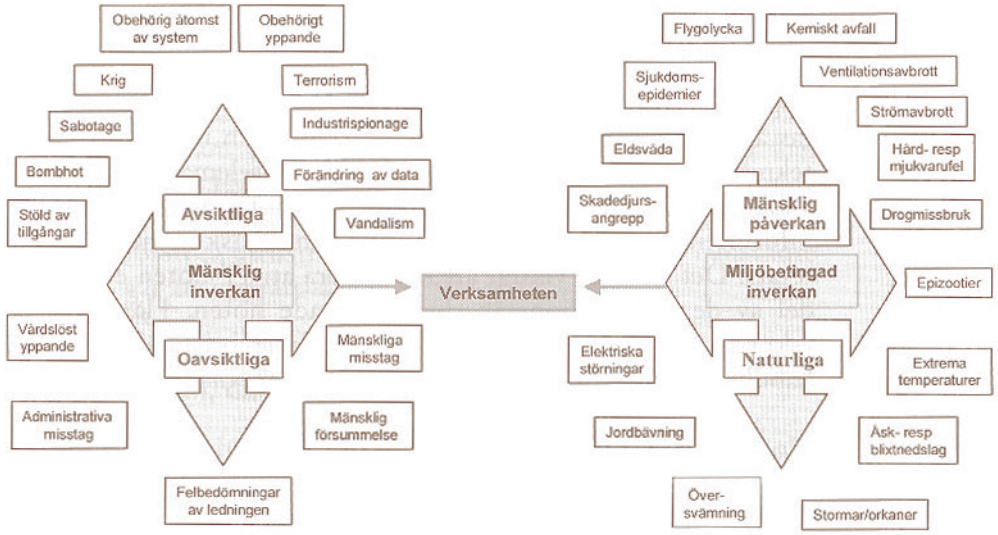
Förutom det område som traditionellt kallats IT-säkerhet så inkluderas även andra begrepp som på olika sätt beskriver hur information ska hanteras på ett säkert sätt i olika typer av organisationer.

”*Utgångspunkten är att viss information kan vara kritisk i något avseende – genom att verksamheten och dess mål kan komma att äventyras om informationen skulle komma till obehörigs kännedom, modifieras, förstöras eller på annat sätt göras otillgänglig”.*

Information i en organisation kan vara olika viktig och kan utsättas för både avsiktliga och oavsiktliga hot. Oavsiktliga hot kan vara slarv av dem som arbetar med den. Informationen måste därför skyddas. De områden som främst påverkats av den snabba teknikutvecklingen vad gäller IT-säkerheten är bl. a. bredbandsutvecklingen, öppen källkod, trådlösa LAN (möjligheter att fysiskt förhindra obehöriga från att använda nätet) och peer-to-peer-nät (spridning av filer infekterade av skadligt slag). Pga. att allt fler ständigt är uppkopplade via bredband ökar risken för olika sorters attacker. Förutom att användarens utrustning är exponerad under en lång tid så kan angriparna även utnyttja klientens höga uppkopplingshastighet. Ett sätt att skydda sig kan vara att man börjar använda program som är baserade på öppen källkod eftersom dessa ger användaren möjlighet att själv kontrollera programmets uppbyggnad, för att där eventuellt kunna upptäcka säkerhetsbrister samt ta bort onödiga funktioner. Nackdelen med öppen källkod är dock att dagens program är väldigt komplexa och att det ofta är väldigt svårt och dyrt att göra en full analys av programmet (SOU 2004:32).

I regeringens proposition Samhällets säkerhet och beredskap, prop. 2001/02:158, beskrivs relationen mellan sårbarhet, hot och risk. Här anser man att risker i samhället bygger på samband mellan olika parametrar, t ex samhällets sårbarhet och möjliga hot. Dessa

parametrar ligger sedan till grund när man utvärderar hur sannolikt det är att en allvarlig situation ska inträffa. Nedanstående modell visar den informationsrelaterade hotbilden.



Figur 3.3 – Hotbild, SOU 2004:32

3.2 *Olyckor och misstag*

Hot som beror på olyckor är i stort sett alltid omöjliga att identifiera innan de plötsligt händer och konsekvenserna är därför även mycket svåra att bedöma. Exempel på olyckor som kan ske är:

- *Ovana användare* kan ställa till med stora problem bland IT-system även om det inte är deras intention. Exempelvis så kan information omedvetet raderas eller så kan det hända att användarkonton inte avslutas efter användning.

- Inte bara ovana användare utan även mer *erfarna användare och systemadministratörer* kan skada och störa system genom otillräcklig kunskap och kompetens. De har ofta inte som motiv att störa eller skada men deras arbetsuppgifter medför att felaktigheter i arbetet leder till just detta.

- *Nyinstallation av program och uppgraderingar* kan ofta vara komplicerade och förutom risken att de anställda i början inte alltid har tillräcklig kompetens om hur programmen ska hanteras på ett korrekt sätt finns även risken att viktig information försvinner i samband med installationen av den nya infrastrukturen.

- *Införande och test av nya system* som kan innehålla oavsiktliga fel i design kan leda till att en tjänst inte fungerar och att data försvinner.

- *Program och utrustning* fungerar ibland inte alltid som den ska och kan leda till att man förlorar information.

- *Olyckshändelser* som *brand och översvämningar* kan leda till att utrustning och information förstörs

(SOU 2004:32).

3.3 Insiderproblem

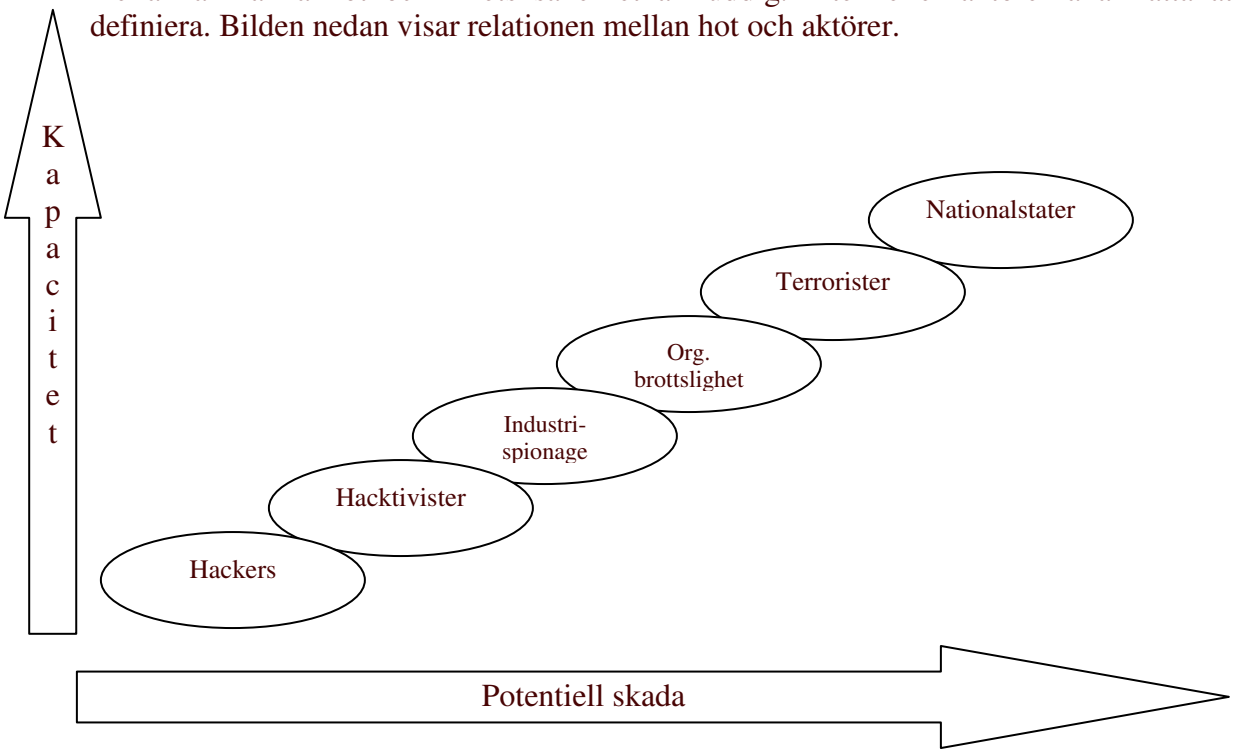
Det är inte ovanligt att de största källorna till informationssäkerhetsproblem är de egna anställa, exempelvis driftpersonal, systemadministratörer, programutvecklare mm. Dessa personer sitter ofta inne med tillräcklig information om brister i systemen och hur dessa kan störas och kan även dela med sig av den informationen till obehöriga utanför företaget. Tack vare enorma möjligheter att kunna spara stora mängder information på olika sorters lagringsmedier är det möjligt att stjäla information utan svårighet. Detta är ofta en personalfråga som är mycket svår att upptäcka och ett hot som sträcker sig ända från rekrytering till efter en anställds avslutande av sin tjänst på företaget. Inte sällan är det personer som känner sig orättvist behandlade som vänder sig emot företaget. Åtgärder kan vara att man har regler och rutiner som personalen följer som stödjer det tekniska säkerhetsarbetet. Andra möjligheter att kontrollera är att ha loggar och olika rättigheter för de anställda (SOU 2004:32).

3.4 Underleverantörer och outsourcing

För att ha en chans att följa med i den snabba teknikutvecklingen och för att spara pengar använder sig många IT-företag av underleverantörer och outsourcing. Detta medför både fördelar och nackdelar. Fördelar kan vara att man får större tillgång till säkerhetsexpertis och enhetligare säkerhetsarbete. Däremot kan outsourcing leda till att det blir svårt att kontrollera hela utvecklingsprocessen. Man kan aldrig vara säker på om säkerhetsföretaget man anlitat har några dolda motiv. Nyttjandet av underleverantörer och övergången till projektorganisationer har ökat den redan stora personalrörligheten inom IT-branschen. Potentiella hot från väldigt kunniga insiders finns ständigt här och man kan inte alltid veta deras motiv. Det kan t ex vara en programmerare som konstruerat ett program och medvetet skapat en bakdörr. Personen kan senare söka anställning hos en organisation som använder sig av det aktuella systemet för att senare utnyttja bakdörren. Problemet är att kontroll som sträcker sig ända från programmering till installation av program i många fall är väldigt begränsad (SOU 2004:32).

3.5 Hotskala

En hacker hackar ofta IT-system för egen räkning för att hävda sig själv och en intellektuell utmaning. Detta får i de flesta fall inte särskilt allvarliga konsekvenser men större hot som uppstått i samband med den allt mer komplexa globala kommunikationsstrukturen kan i värsta fall äventyra rikets säkerhet. Var gränsen går mellan allmänna hot och rikets säkerhet är luddig. Inte heller aktörerna är lätta att definiera. Bilden nedan visar relationen mellan hot och aktörer.



Figur 3.4 – Hotskala, Egen efter SOU 2004:32

Stater har övergripande politiska och långsiktiga strategiska mål. Terrorister kan antas ha någon form av politiska eller religiösa mål medan den organiserade brottsligheten i huvudsak kan tänkas drivas av egenintresse. Även vad gäller industrispionage är det i de flesta fall egenintresse som är drivkraften fast här är det främst riktat mot konkurrenter. Vad gäller hacktivister, t ex olika politiska grupper, kan de tänkas styras av att driva de egna frågorna som de förespråkar. Sista kategorin i modellen är då de enskilda hackers vars syfte redan beskrivits. Hackers kan delas in i tre kategorier: White hat, Black hat och Script kiddies. White hat-gruppen är kompetenta individer som använder sina kunskaper för att hitta säkerhetsluckor och brister i system för att sedan sprida denna information vidare. Black hat-gruppen är minst lika kompetenta men arbetar med andra system, såsom att krascha system, stjäla användaruppgifter från hackade system och skapa och sprida virus. Script kiddies har inte samma kunskaper om hacking men pga. färdiga tool kits som man nu enkelt kan finna på nätet lyckas dessa personer skapa minst lika stora problem som de två andra grupperna. Hackers kan använda sig av olika metoder för att få reda på svagheter i organisationens system. Vanligaste sättet är att man tar kontakt med en anställd, t ex att man ringer kundsupport och utger sig för att vara en anställd på

företaget och ställer där frågor som kan avslöjar svagheter. Hackern kan även besöka företaget fysiskt som kund för att där ställa frågor till anställda för att på samma sätt lära känna systemen och rutinerna. Det här sättet kallas för social engineering. För att skydda sig mot detta räcker det inte att förlita sig på tekniska system utan det är minst lika viktigt att klara policies och direktiv har getts till de anställda om hur det ska reagera i olika situationer och vilka frågor man får besvara och hur.

En annan viktig faktor är tidsförhållandena. Vissa attacker kan vara väldigt snabba att genomföra men svåra att nå de specifika målen samt att kontrollera spridningen efteråt. Ett exempel på dessa är datavirus. För att effektivisera en attack krävs det att man noga undersökt systemet och lärt känna det innan, vilket både tar lång tid och kostar mycket (SOU 2004:32).

3.6 *Hackermetoder*

Tidigare kapitel inom begreppteorin handlar om övergripande problem inom IT-säkerhet. Nedan förklaras konkreta och faktiska metoder att angripa ett IT-system.

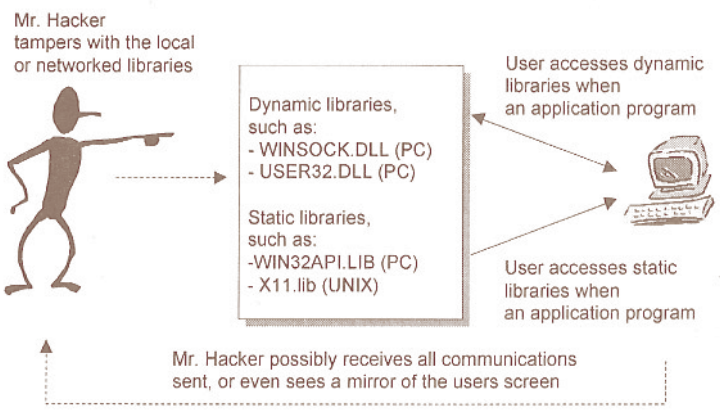
IP-spoofing är när en angripare stjäl en IP-adress för att genom användning av denna få åtkomst till områden som är begränsande till vissa IP-block. Eller låtsas vara någon annan i likartade syften. Vad som sker i dessa attacker är att angriparen inväntar att den dator som besitter den önskade IP-adressen inte används. När datorn inte används stjäl hackern denna IP-adress (Buchanan 1999, Cisco Systems 1999).

Buffer overflows inträffar när ett program på något vis skriver mer minne än vad som finns allokerat. Buffer overflows inträder ofta till följd av en bug i program skrivna i assembly language, C eller C++, som inte är minnessäkra. Programspråk som Java hanterar minnesallokering automatiskt och använder run time checking och static analysis att göra det omöjligt eller mycket svårt att koda en buffer overflow bug (Länk 1).

Application-Layer attacks finns i flera olika former. Den vanligaste är exploatering av kända svagheter i mjukvara som ofta finns på servrar såsom sendmail, PostScript och FTP. Genom att exploatera dessa program kan angriparen få tillgång till systemet som kör applikationen med rättigheterna som kontot har som kör processen. Ofta har konton som kör dessa applikationer privilegierade systemnivåsrättigheter vilket leder till att systemet blir mycket sårbart om angriparen kommer över detta. Java applets och ActiveX controls är HTTP funktioner som kan utnyttjas på samma sätt (Cisco Systems 1999).

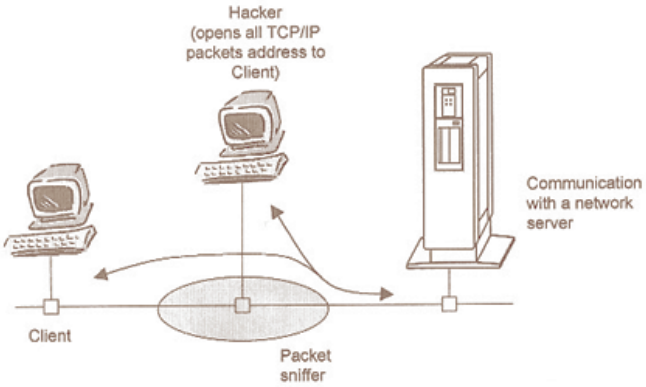
Denial-of-Service attacks fortkortat DoS attacker, skiljer sig från andra angrepp i den mening att attackeraren inte har för avsikt att få tillträde till ett nätverk. Denna attack fokuserar sig på att störa en nätverkstjänst som är i drift. Detta kan vara en webserver, mailserver, dnsserver, ftpserver osv. För att uppnå detta mål kommer angriparen att överbelasta servern så att åtkomst till den inte är möjlig (Cisco Systems 1999).

Shared library attacks. Många system har ett område med delade library files, på svenska, delade systemfiler. Dessa filer kallas av applikationer när de behövs för exempelvis input/output, nätverksåtkomster, grafik osv. Vid tillfälle kan en angripa ersätta dessa systemfiler med egna versioner av filen. Denna ersatta fil har samma egenskaper som originalet (Buchanan 1999).



Figur 3.5 – Shared library attack (Buchanan 1999)

Packet sniffing är ett begrepp som används när en angripare lyssnar på TCP/IP paket som skickas ur ett nätverk. Vad man vill göra med denna information är varierande. Information som brukar vara av intresse är användarnamn, e-mail, bankkontonummer, kredit kort osv. Denna metod används innan IP-spoofing för att få information om servrar klienten är i kontakt med. Många TELNET och FTP program skickar användarnamn och lösenord som textsträngar vilket lätt kan uppsnappas med hjälp av packet sniffing (Buchanan 1999).



Figur 3.6 – Packet sniffing (Buchanan 1999)

Password attacks. En vanlig svag länk i alla system. Det angriparen gör är att leta efter användare med svaga lösenord, speciellt användare som har samma login och password. Annars använder sig angriparen av program som försöker ”gissa” lösenordet genom att den kör cykler med olika kombinationer av ord. Det värsta som kan hända i detta fall är att angriparen kommer över lösenordet för systemadministratören (root) (Buchanan 1999, Cisco Systems 1999).

Social engineering attacks riktas till användare som har liten förståelse kring sitt datasystem. En variant av denna attack är att man ringer upp en användare inom ett nätverk per telefon (gärna en interntelefon) och utger sig för att vara systemadministratör. Därefter ber man om användarens lösenord. En vanlig användare på ett nätverk har sällan en uppfattning om hur en systemadministratör sköter sitt arbete och kan således tro att det rör sig om ett genuint administratöruppdrag (Buchanan 1999, Cisco Systems 1999).

Technologial vulnerability attacks är likt Application-Layer attacks och involverar en attack på en specifik del av systemet. I detta fall är det regelmässigt operativsystemet som attackeras. Angriparen siktar in sig på en svaghet i operativsystemet och utnyttjar denna för att få åtkomst till systemet (Cisco Systems 1999).

3.7 *Malicious Software*

Malicious software (på svenska direktöversatt till ondsint mjukvara) omfattar ett flertal olika programformer. Som namnet antyder är programmet ute efter att skada systemets innehåll eller kränka den personliga integriteten.

3.7.1 Virus

Ett virus är ett program som kan infektera andra program och modifiera dem. Biologiska virus är små bitar av genetisk kod, DNA eller RNA som kan ta över mekaniken hos en levande cell och lura den att skapa tusentals kopior av viruset. På samma vis fungerar ett datoriserat virus (Stallings 2003). Vad viruset har för uppgift varierar ofta, därav uppkomsten av många nya begrepp och namn.

3.7.2 Spionprogram

Citat hämtat från Post och Telestyrelsen (PTS-ER-2005:15).

> ” Spionprogram eller spyware försöker samla information om dina vanor. Oftast är de ett större hot mot användarens personliga integritet än mot dator som sådan. Spyware laddas ofta ner tillsammans med något annat program utan att användaren vet om det eller är medveten om vad hans/hennes agerande innebär. Programmet samlar sedan information om användarens Internetvanor och skickar den till externa mottagare.”

Som citatet anger är hotet främst mot personlig integritet och inte mot data. Ett spionprogram kan kompletteras med trojanska hästar som förklaras i rubriken nedan.
Den form av spionprogram som författarna anser är allvarligast är Keyloggers.

3.7.3 Keyloggers

Moderna keyloggers sparar inte bara tangenttryckningar som namnet antyder utan kan även spara skärmdumpar då den får träff på valda nyckelord som skrivs eller visas på skärmen. Eller så är programmet helt gjort för att spara användarnamn och lösenord (PTS-ER-2005:15).

3.7.4 Trojanska hästar

Trojanska hästar är malicious code (illvillig kod) som läggs till ett befintligt program och exekverar kod som användaren är omedveten om. NE (Länk 2) definierar det som en dold funktion i ett program som användaren inte hade exekverat om man varit medveten om den. Målet med en trojansk häst är att öppna ett hål i offrets säkerhetsanordning som sedan kan utnyttjas för olika ändamål. Det kan vara att fjärrstyra datorn eller skicka filer från offrets dator.

3.7.5 Worms (Maskar)

En worm (på svenska mask) har som primära avsikt att sprider sig vidare. Detta gör den med hjälp av säkerhetshål eller genom email. Det är detta som gör att maskar kan sprida sig så otroligt fort. En snabb mask tar så lite som 5 timmar på sig att sprida sig över hela världen (Länk 3).

Den stora skillnaden mellan en mask och ett virus är sättet att infektera. Ett virus försöker förstöra så mycket som möjligt i en och samma dator medan en mask försöker smitta så många andra som möjligt och utföra någon liten ändring i systemet som är smittat. Många som skriver maskar och malicious software gör det i förhoppningen att just deras programkod skall bli så stor att den omnämns i nyhetsbrev på Internet och i tryckta tidningar (PTS-ER-2005:15).

Stallings (2003) definierar skillnaden mellan ett emailvirus och en mask med att ett virus måste skickas av en människa. En mask sprider sig utan den smittades vetskap.

3.8 *Brister inom applikationer*

En anledning till att nätverk ständigt är sårbara mot angrepp är att applikationer blir allt mer invecklade. Tim Keanini (2005) skriver i sitt paper att det finns tre kategorier eller errors som bidrar till sårbara nätverk.

- Design error.
    - Fel i applikationen.
- Implementation error.
    - Fel som uppkommer i implementationen. Löses med en patch.
- Configuration error.
    - Konfigurationer som orsakar sårbarheter.

Dessa sårbarheter utnyttjas av Buffer overflow hacks (design error) och Application layer attacks (Design error, Implementaion error och Configuration error).

3.9 *Åtgärder mot IT-hot*

Följande underrubriker handlar om faktiska åtgärder, i form av mjuk- och hårdvara, för att skydda sig mot IT-relaterade hot.

3.9.1 Firewalls

En anslutning till Internet medför två nackdelar för organisationer.

- Möjlighet för användare att utnyttja icke arbetsrelaterade applikationer.
- Tänkbara anslutningar från det globala nätverket (Internet) till sitt eget nätverk som ej är önskvärt.

På grund av den sistnämnda anledningen har organisationer valt att skärma av sina nätverk (intranät) från Internet. Dessa in-house intranät kan blockera utgående trafik (all trafik eller specificerad trafik) och kan blockera ingående trafik (all trafik eller specificerad trafik). Detta med hjälp av firewalls, på svenska brandväggar. Brandväggar finns i både mjukvaru- och hårdvaruform. En mjukvarubrandvägg kan installeras direkt på datorn medan en hårdvarubrandvägg är en fysisk apparat. En brandvägg kan filtrera trafik på olika sätt beroende på vad man vill åstakomma med den.

IP begräsning – Endast tillåta inkommande trafik från vissa IP block eller domäner.
Portblockad – Stänga vissa portar för inkommande/utgående trafik.
Blockera ord och fraser – Brandväggen kan sniffa paketen och förbjuda vissa typer av fraser och ord att komma igenom (Panko 2003, Buchanan 1999).

3.9.2 IP security (IPsec)

Pankos (2003) beskrivning av IPsec.

Till skillnad från SSL (Secure Sockets Layer) som fungerar på transportskiktet (transport layer) så tillhandahåller IPsec även säkerhet på internetskiktet (internet layer) i TCP/IP arkitekturen. Detta medför att all trafik över TCP och UDP kan skyddas. IPsec var

konstruerat att användas med Internet Protocol version 6 (IPv6) men den går även att använda på IPv4. Det grundläggande konceptet med IPsec är de två olika sätten det används, transport mode och tunnel mode.

Transport mode används för värd-till-värd säkerhet. Transport mode tillåter två värdar att kommunicera säkert utan att störas av vad som händer på nätverket. En IPsec header sätts in efter huvud-IP headern. Denna IPsec header kommer att tillhandahålla säkerhet för transport och applikationsskikten. Dessvärre måste IP headern skickas okrypterad vilket medför att någon som sniffar trafiken kan se vilken IP-adress som mottagaren har.

I kontrast med transport mode används tunnel mode för säker kommunikation mellan två IPsec servrar. Dessa servrar skickar trafik mellan varandra över Internet genom säkra ”tunnlar”. I tunnel mode är hela original IP headern skyddat. Den överförande servern kapslar in original IP headern i en ny IP header och en IPsec header. Att kapsla in ett protokollmeddelande med ett annat protokollmeddelande i samma skikt kallas att tunnla. Destinationen på den nya IP headern blir således IPsec servern på andra ändan. Denna server kommer i sin tur ta emot headern och packa upp den och skicka vidare originalheadern till mottagaren som sitter bakom den mottagande IPsec servern. På detta vis spelar det ingen roll om någon snappar upp paketen på vägen. De visar ändå bara IP destinationen till en IPsec server och inte den egentliga mottagaren till paketet.

3.9.3 Kryptering

Kryptering är en metod för att säkerställa att data som skickas är autentisk. Det finns två olika former av kryptering som finns i vardagligt bruk, konventionell kryptering även kallad symmetrisk kryptering och public-key kryptering även kallad asymmetrisk kryptering (Stallings 2003).

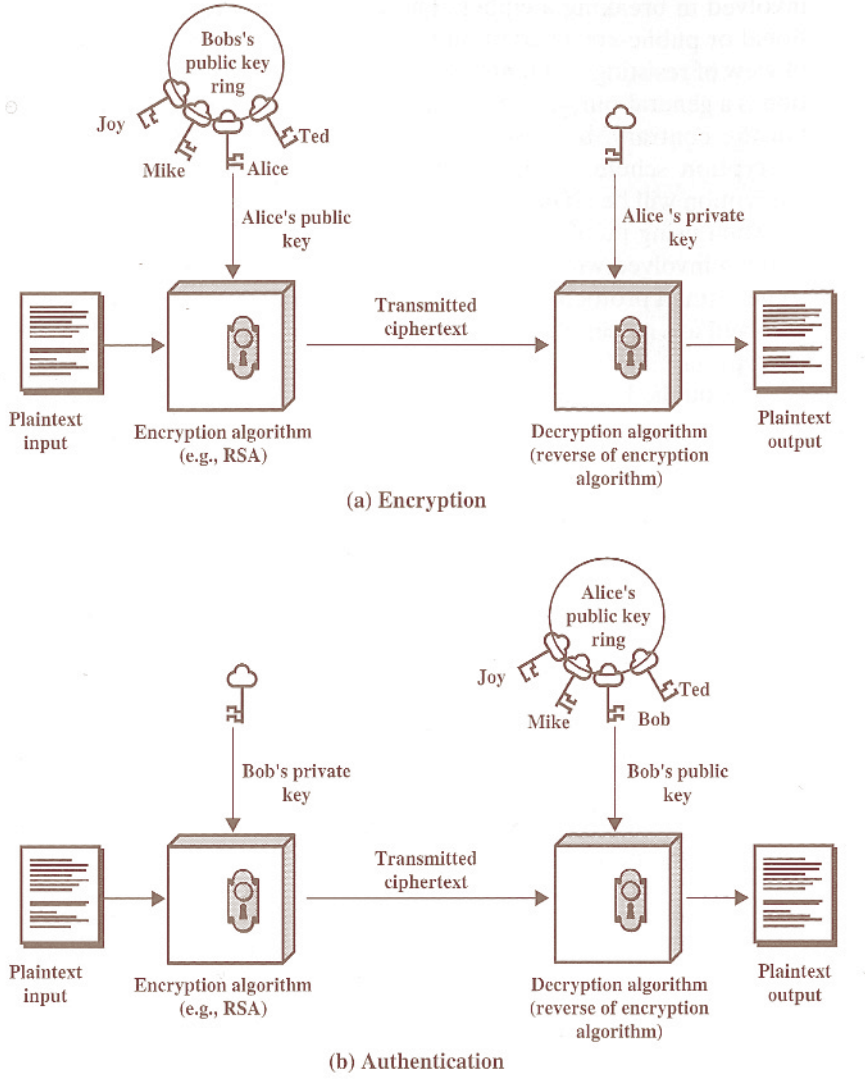
3.9.3.1 Symmetrisk kryptering

Symmetrisk kryptering består av fem steg. I symmetrisk kryptering delar man på en hemlig nyckel som används för att kryptera och kryptera upp data.

- *Plaintext*. Originalmeddelandet eller data som skickas som input in i algoritmen.
- *Krypteringsalgoritm*. Algoritmen genomför vissa substitutioner och transformationer på plaintextmeddelandet.
- *Hemlig nyckel*. Denna nyckel läggs in som output i algoritmen. Vilka substitutioner och transformationer som sker är beroende på nyckeln.
- *Ciphertext*. Meddelandet eller data i krypterad form.
- *Dekrypteringsalgoritm*. Samma algoritm och nyckel används som i tidigare steg men baklänges för att få ut ciphertexten i läsbar plaintext (Stallings 2003).

3.9.3.2 Asymmetrisk kryptering

Denna form av kryptering skiljer sig från ovanstående i den mening att krypteringen bygger på två nycklar. En publik nyckel och en privat. Figurer nedan demonstrerar hur krypteringen och autentisering går till. Användare A skickar ett krypterat meddelande till använde B genom att använda Bs publika nyckel. Användare B använder sin privata nyckel för att kryptera upp meddelandet (Stallings 2003).



Figur 3.7 – Public-Key Cryptograpy (Stallings 2003)

3.9.4 Intrusion detection

Intrusion detection är processen att övervaka datornätverk och system för brott mot säkerhetspolicyn som är gällande. I enkla termer består intrusion detection av tre komponenter.

- En informationskälla som tillhandahåller ett flöde av händelserapportering.
- En analytisk motor som hittar spår av intrång.
- En komponent som genererar åtgärder baserad på den analys som motorn har gjort.

3.9.4.1 Mål med intrusion detection

En faktor inom intrusion detection är vilka mål som processen stödjer. De två traditionella målen som driver intrusion detection är ”accountability” och ”active repsonse”.

Accountability är förmågan att kunna kartlägga en aktivitet på systemet tillbaka till den personen ansvarig. Slutgiltiga målet med detta är att kunna erhålla någon form av ersättning eller gå vidare med ärendet till myndigheterna. I och med detta blir denna metod effektivare om man kan spåra handlingen till en person och inte ett datornamn eller IP-nummer. Att ha denna funktion fungerande på ett nätverk ses som en av de stora utmaningarna inom intrusion detection. När en attack använder program och daemons på separata maskiner får varje anslutning en egen identitet. Desto fler anslutningar som används desto lägre är sannolikheten att intrånget kan upptäckas och spåras för att sedan uppnå accountability.

Response är när en analys frambringar ett händelseförlopp vid ett intrång (eller vad sitt system har för avsikt att reagera på). Response är inte begränsad till att bara påbörja åtgärder mot intrånget, vilket namnet tycks insinuera. Den förmodligen vanligaste formen av response är att spara analysen i en log fil och sedan använda denna för att generera en rapport. Denna information är av intresse för många parter inom en organisation och genererar olika former av detalj beroende på vem som skall läsa den. En systemadministratör får förhoppningsvis en väldigt detaljerad beskrivning av vad som har skett med information om intrånget, vilka filer som har berörts av intrånget osv. Ledningen å andra sidan får endast information om hur många intrång som ägt rum och hur allvarliga dessa har varit.

En mer direkt form av response är att utlösa någon form av larm av varierande slag beroende på hur allvarligt intrånget är. Dessa larm inkluderar en flagga i nätverksadministratörens konsol, ett meddelande på en säkerhetsansvarigs personsökare eller helt enkelt ett e-mail som skickas till den som övervakar systemet.
En annan repsonse-åtgärd är att konfigurera om systemet som har utsatts för intrång. Detta skulle kunna vara att skrivskydda filer som systemet anser är under hot. Att kunna anpassa sitt system efter denna metod gör säkerheten flexibel och inte statiskt fast vid förutbestämda åtgärder.

Den response som återstår är den mest kontroversiella. Detta är strike-back. Med denna metod blockerar man intrånget genom att spegla intrånget/attacken tillbaka till källan den kom från. En mer godartad form av strike-back är att skicka meddelanden till

brandväggar och routrar om att blockera nätverksåtkomst från den källa man anser ger sig på ett intrång eller en attack mot sitt system (Bace 2000).

3.10 *Verktyg för att förebygga brister inom IT-säkerhet*

Vi har i förgående kapitel berättat om mjukvara för att skydda sig mot IT-hot. Här nedan förklaras processverktyg och en ISO standard som används för att implementera en fungerade säkerhetspolicy.

3.10.1 ISO-standarden 17799

ISO 17799 är en internationell standard som började som brittisk standard i mitten av 1990-talet. Den hette då BS 7799. Standarden handlar om informationssäkerhet på ledningsnivå och består av tio olika delar:

- Security Policy
- Security Organization
- Assets Classification and Control
- Personnel Security
- Physical & Environmental Security
- Communications & Operations Management
- System Access Control
- Systems Development & Maintenance
- Business Continuity Planning
- Compliance

SIS, Sveriges Standard Institute, beskriver ISO 17799 så här:

> ”Riktlinjerna i standarden ger rekommendationer för ledning av informationssäkerhetsarbetet för de som ansvarar för att initiera, införa och underhålla säkerhet i sina organisationer. De är avsedda att ge en gemensam grund för organisationer att upprätta ett effektivt ledningssystem för informationssäkerhet som bidrar till ett ökat förtroende för organisationen internt och externt. Rekommendationerna i denna standard bör väljas och tillämpas i enlighet med gällande lagar och förordningar.”

Standarden dök först upp 1995 i form av praktisk kod hur vissa saker skulle skötas inom området. Av diverse anledningar så fick den ingen större genomslagskraft då. Det var först efter 1999 när version 2 släpptes som den slog igenom i samband med att ett antal hjälpverktyg till dem presenterades. Standarden blev inte officiell förrän i december år 2000. Användandet av standarden har ökat explosionsartat och efter att fler och fler företag bestämt sig för att använda sig av den ses den numera som den huvudsakliga och absolut ledande standarden inom Informationssäkerhet. Anledningen till att den fick så stor genomslagskraft på senare tid beror mest på att E-business och behovet av en säker miljö har ökat. Många större företag har investerat stora summor pengar för att förbättra

kvalitén på ISO 17799 och även att tidigare hot såsom Y2K har försvunnit eller blivit lösta. Eftersom kravet på en säker organisation har blivit så tydligt så har ISO 17799-certifierade företag en enorm konkurrensfördel gentemot konkurrerande företag som kanske bara använder sig av sina egna policys. När man som företag ska bestämma sina säkerhetspolicys har man fyra val. Man kan antingen helt strunta i ISO 17799 eller så kan man basera sina policys på ISO 17799 och endast ha dessa som riktlinjer. Tredje alternativet är att man helt ser till att ens policys stämmer överens med ISO 17799. Det bästa alternativet är dock att man ansöker om att få en ISO 17799-certifiering (Länk 4, SOU 2004:32)

3.10.2 SBA Check

SBA Check arbetar med hjälp av olika checklistor som är en värdefull del av säkerhetsarbetet och hjälper organisationen leva upp till övergripande krav. IT-konsulten Hans Husman skriver i sin artikel (Länk 5) om verktyg för informationssäkerhet. Efter diverse tester ges SBA Check betyg 4/5 och hamnar därmed på andra plats efter PAPAI av de tre verktygen som jämförs (SBA Check, SBA Scenario och PAPAI). SBA Check inkluderar checklistor för 7799, FA22, två stycken för PUL och en generell checklista för nulägesanalyser av informationssäkerhetsstatusen. Författaren anser att SBA Check är bra men otillräckligt för större företag.

3.10.3 SBA Scenario

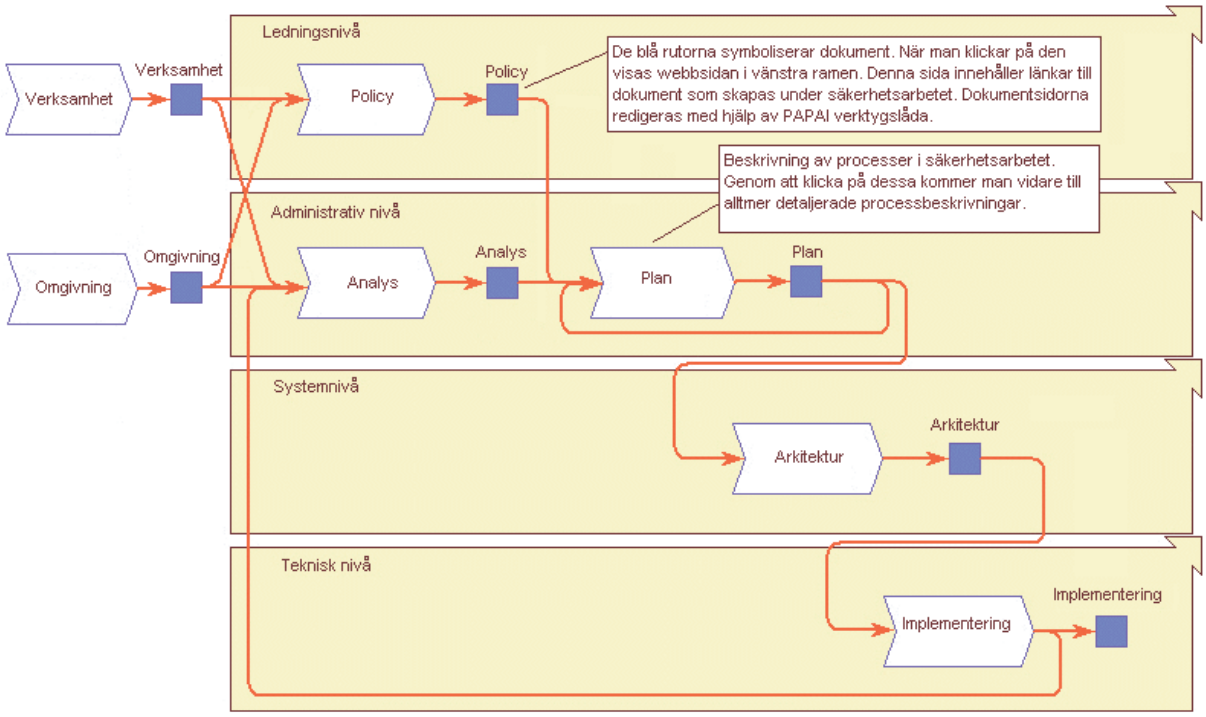
SBA Scenario är ett verktyg som hjälper till analysera scenario som påverkar ett företags resurser. När man ska skapa ett nytt scenario fyller man i data av olika typer, t ex analysledare, system som analysen görs på, de personer som deltar i analysen, brister med uppskattat skadekostnad och sannolikheten att en händelse kan inträffa under året. Utifrån detta kan man sedan ta fram bra sammanfattande rapporter. Ur artikeln framgår det att verktyget är bra på så sätt att det automatiskt ger ett strukturerat och bra arbetssätt. Däremot det får kritik för det höga priset och att större företag oftast redan har metodstöd, som i många fall mer än väl täcker upp det som SBA scenario erbjuder. Verktyget får därför endast en tvåa i betyg. Verktyget är enligt IT-konsulten Björn Ivarsson bra på att i ett tidigt skede skildra och tydligt klargöra för informationssäkerhetsansvariga hos företag vad deras brister kan komma att kosta om inte förbättringar inom dessa områden görs (Länk 5, diskussionsmaterial med Björn Ivarsson).

3.10.4 PAPAI

Det verktyg som fått bäst betyg (Länk 5) och används i störst grad är PAPAI, som står för: Policy, Analys, Plan, Arkitektur och Planering och är ledningssystem för informationssäkerhet. Detta system är ett komplett verktyg för både IT- och informationssäkerhetsarbete.

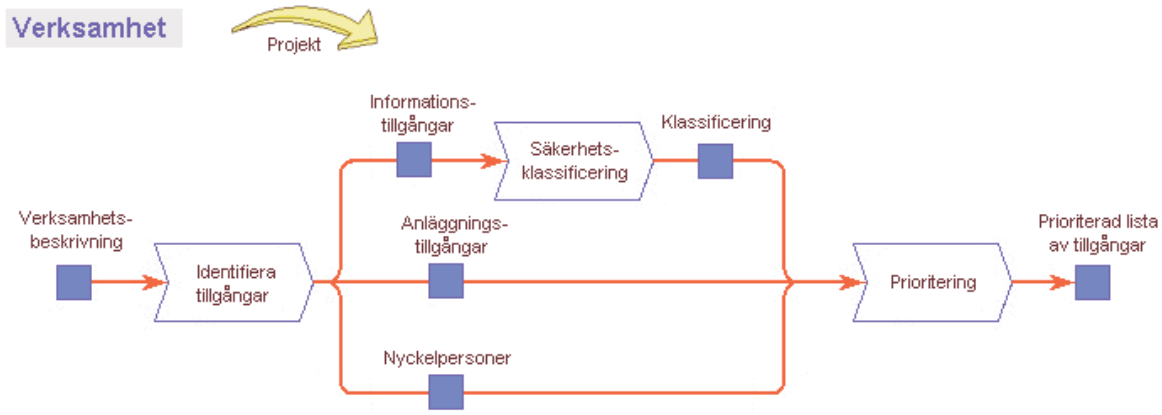
”Syftet med PAPAI-konceptet är att ge ett praktiskt stöd och ett färdigt ramverk för säkerhetsarbetet. Metoden åskådliggörs grafiskt på ett antal webbsidor som uppdateras under arbetets gång och bildar ett processorienterat ledningssystem för informationssäkerhet. Till detta hör ett stort antal mallar, checklistor, projektaktiviteter mm. Dessa används som utgångspunkt i det egna säkerhetsarbetet och gör det möjligt att snabbt ta fram egna policies, riktlinjer och annan dokumentation som också läggs in i den färdiga PAPAI-strukturen (Länk 6)”.

Arbetsmetodiken börjar i den aktuella verksamhetens krav och går hela vägen ner till implementeringen. Aktiviteterna i PAPAI anpassade för att tillgodose de krav som ställs av bl.a. BITS (basnivå för IT-säkerhet) och ISO/IEC 17799. De olika aktiviteterna delas upp i fyra olika organisationsnivåer. Den översta nivån är ledningsnivån. Här resulterar verksamhetens krav i en säkerhetspolicy. Nivån under är den administrativa. Där görs ett analysarbete, som dels påverkas av den tekniska nivån och verksamhetens krav från den understa nivån, dels av omvärlden. Sedan gör man en plan för företagets/organisationens säkerhetsarbete, baserad på denna analys. Sedan utvecklar man arkitekturen för alla säkerhetsfunktionerna, vilket görs på systemnivån med hjälp av den framtagna planen. I den lägsta nivån finns den tekniska biten. Här sköts implementeringen och den görs enligt arkitekturen. För varje aktivitet i verktyget kan man göra finjusteringar genom att steg för steg klicka sig vidare till undernivåer för att specificera. Eftersom verktyget är så flexibelt och lätt att anpassa till den egna verksamheten kan det användas även för andra aktiviteter i verksamheten. Vill man t ex att anställda ska göra vissa säkerhetsaktiviteter när produkter köps in eller system ska utvecklas kan detta läggas in i PAPAI. En annan fördel med PAPAI är att man kan komplettera befintlig data med egna dokument, köpa till fler paket, lägga till checklistor och information om kontaktpersoner. Presentationen sker via webbsidor, vilket gör att verktyget även fungerar bra t ex på ett företags intranät. Det är fördelaktigt eftersom alla anställda då med enkelhet kan surfa in och ständigt hålla sig uppdaterade på policys, riktlinjer, checklistor med mera. En annan fördel med PAPAI är att man själv kan bestämma vilka paket av PAPAI man vill köpa in. Ett lite mindre företag kanske nöjer sig med att köpa in grundpaketet medan ett större företags kanske vill säkerställa IT-systemet genom att köpa alla tilläggspaket. Nedan följer en lite utförligare beskrivning av PAPAI:



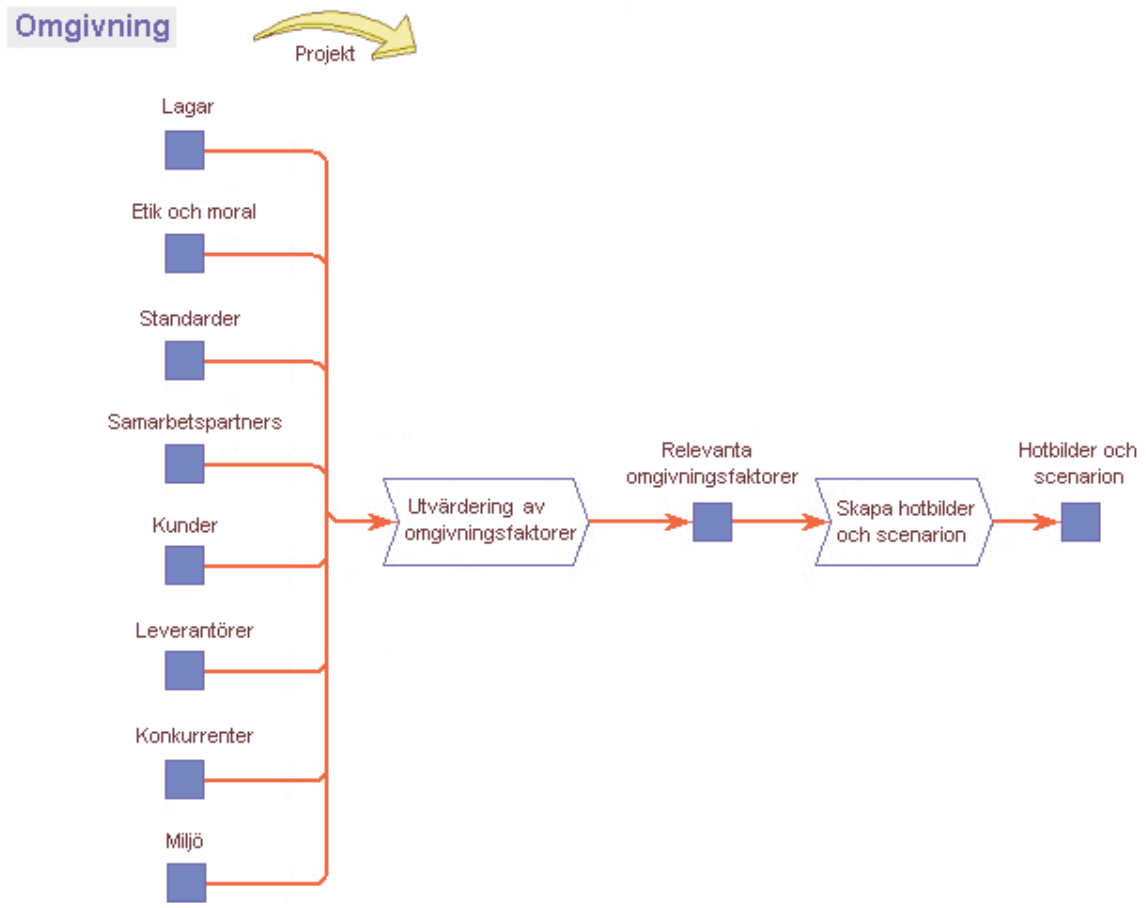
Figur 3.10 – Översikt, Länk 6

Så här ser huvudfönstret i PAPAI ut med dess sju olika kategorier som definieras i tur och ordning. Alla rektangulära kategoriknappar är klickbara för ytterligare fördjupning och finjustering. I det första steget beskrivs verksamheten. Det handlar främst om att identifiera olika typer av tillgångar, såsom informationstillgångar, anläggningstillgångar och nyckelpersoner. Slutprodukten av det här steget blir en prioriterad lista av företagets tillgångar. Nedan följer en bild på de olika stegen i verksamhetsanalysen:



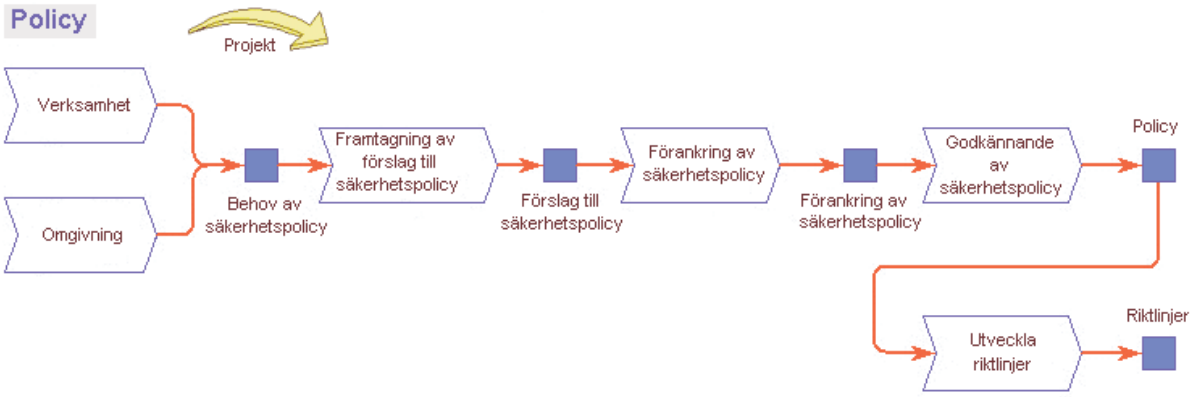
Figur 3.11 – Verksamhet, Länk 6

I nästa steg, omgivningsanalysen, definieras bl.a. företagets kunder och samarbetspartners, lagar, etik och moral samt diverse standarder.



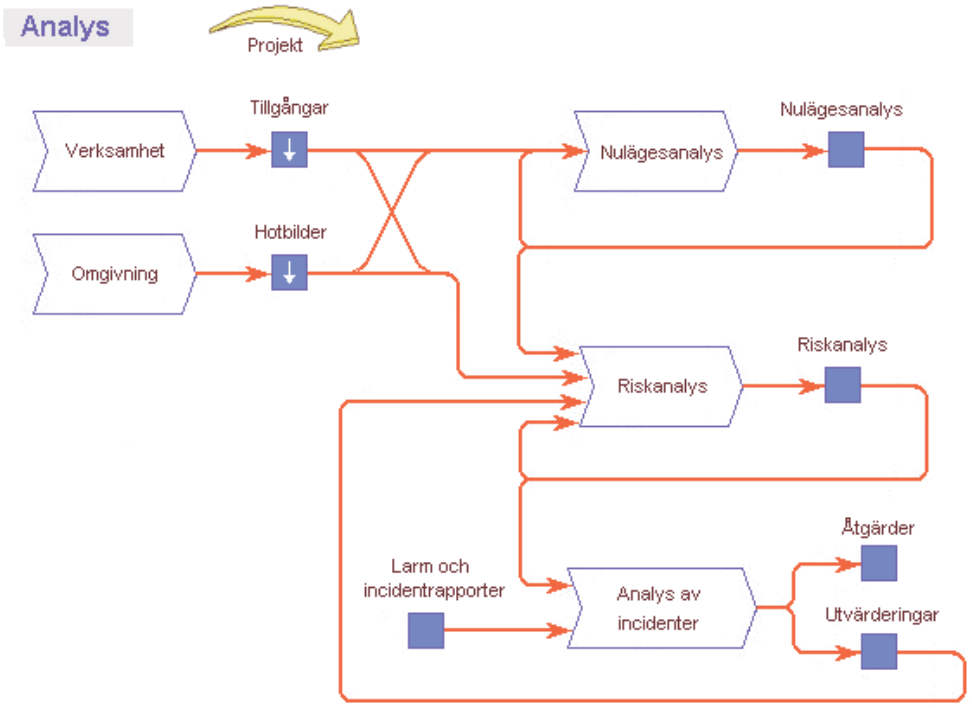
Figur 3.12 – Omgivning, Länk 6

Efter att ha analyserat företagets olika tillgångar och omgivning börjar man med att skapa och förankra en säkerhetspolicy och riktlinjer. PAPAI hjälper här till med bl.a. projekthandledning och projektaktiviteter till policyprojektet, mallar för övergripande säkerhetspolicy, presentationer för förankring av policyarbetet för ledningen och de anställda samt exempel på riktlinjer.



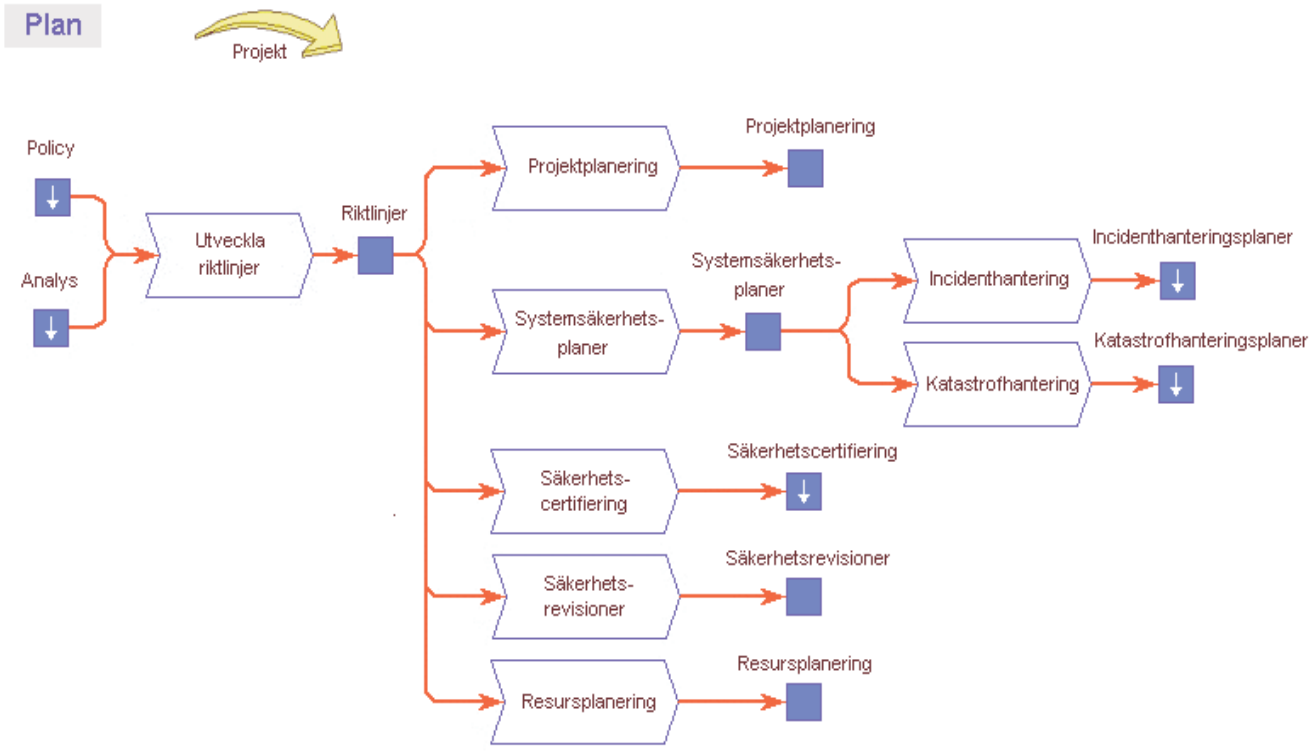
Figur 3.13 – Policy, Länk 6

Nästa steg man gör är olika analyser, bl.a. nuvärdesanalys, riskanalys och analys av incidenter. Nulägesanalys kan ske via en checklista eller med hjälp av programvara.
Denna checklista medföljer i paketet för riskanalysen. I nuvärdesanalysen jämförs företagets säkerhetsstatus mot ISO-standarden 17799 eller mot BITS, beroende på vilken standard man vill följa. En grundanalys som utgår från kundens krav är grundläggande för hela säkerhetsarbetet. Den här delen ligger till grund för planeringsfasen där man bestämmer de mest kostnadseffektiva säkerhetsåtgärderna. När man gör analyserna använder man sig av mallar som beskriver verksamhetens tillgångar samt hoten mot dessa och dess egenskaper. Man använder sig även av en checklista för säkerhetsrutiner och en för nulägesanalysen.



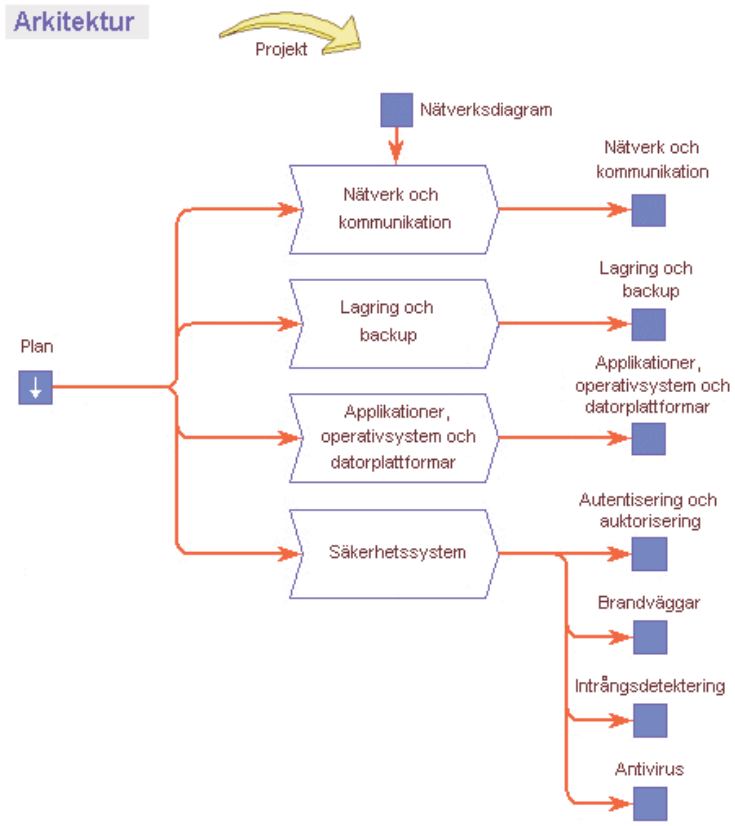
Figur 3.14 – Analys, Länk 6

Efter analysfasen går man in i plan-stadiet. Här utvecklas bl.a. riktlinjer, projektplanering, säkerhetscertifiering, resursplanering samt incident- och katastrofplanering. Det här steget ger stöd för att följa BITS, som har skapats av Krisberedskapsgruppen (KBG). I BITS har en säkerhetsnivå definierats som *minst* måste uppnås för samhällsviktiga IT-system som bedöms vara nödvändiga för att en verksamhets normala förhållande även under fredstida kriser. I Plan-stadiet använder man sig bl.a. av mallar policy för katastrofberedskap, arkiveringsplan, underhållsplan samt åtgärder vid katastrof. Nedan presenteras menyn för Planfasen:



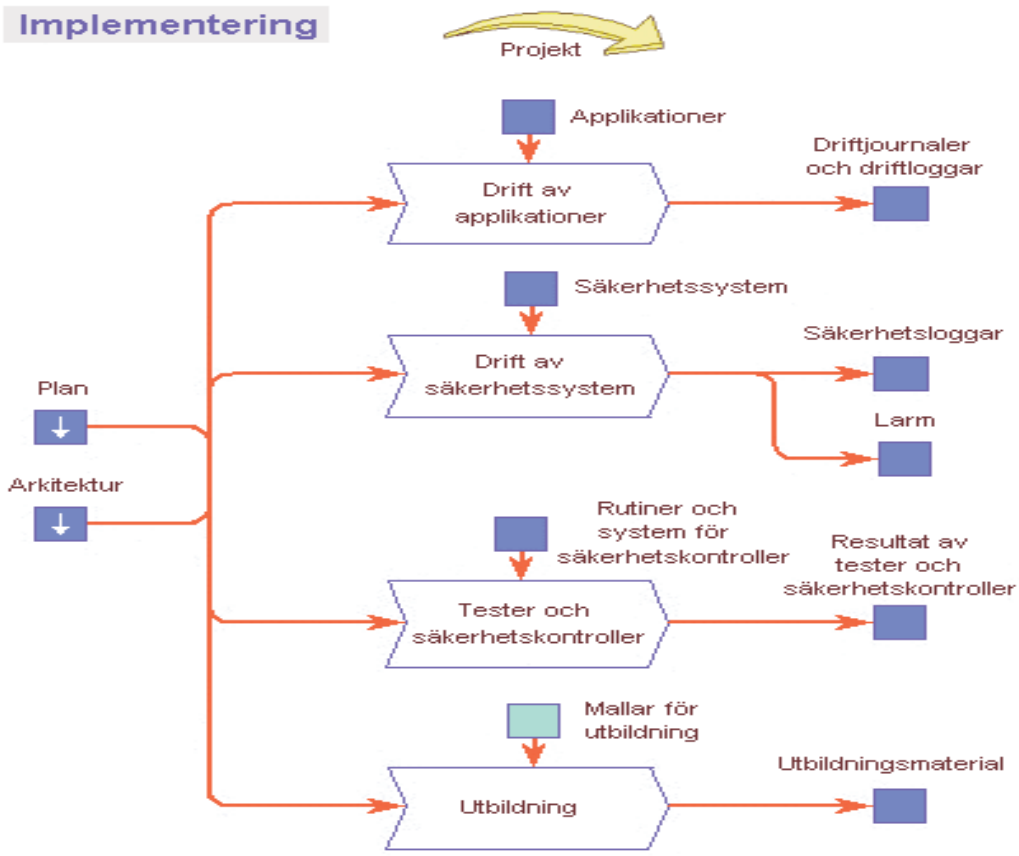
Figur 3.15 – Plan, Länk 6

När man har fullbordat planfasen börjar man arbeta med arkitekturen. Här gör man indelningar i säkerhetsdomänen och säkerhetszonen. Säkerhetsdomänen är det område som man har inflytande över medan en säkerhetszon är ett antal nätverk, arbetsstationer, servrar mm som omfattas av samma säkerhetsregler. Förutom att principer för datalagring och backup görs här så sätts även säkerhetsregler för autentisering och auktorisering för användare här. Även val av brandväggar, IDS (Intrusion Detection System) och virusprogram definieras i det här stadiet.



Figur 3.16 – Arkitektur, Länk 6

Sista steget i PAPAI är implementeringen. Här görs bl.a. Penetrationstester, kontroll av konfigurationer, loganalys. Slutligen kommer man till ett av de absolut viktigaste stegen i hela arbetet nämligen utbildning av personal. Det rör sig då om personer i ledningen, användare och driftpersonal. Sammanfattningsvis kan man säga att PAPAI hjälper företag att komma till rätta med sina administrativa säkerhetsbrister. Att bygga ett LIS är inget man gör på några dagar utan ett långsiktigt arbete som ska få alla inom organisationen att jobba kontinuerligt med informationssäkerhet. Målet med att bygga ett LIS (ledningssystem för informationssäkerhet) är inte alltid att bli certifierad mot ISO 17799 utan att höja säkerhetsmedvetandet inom organisationen och på så sätt spara pengar när väl någon incident eller katastrof inträffar (Länk 6, Länk 7, diskussionsmaterial från Björn Ivarsson.)



Figur 3.17 – Implementering, Länk 6

3.10.5 Proactive Network Security

Tim Keaninis (2005) framhäver i sitt paper att man genom fem steg kan ha en heltäckande strategi inom IT.

> ”Proactive network security offers a new strategy by combining five key elements: (1) detailed assessment of all devices on the network; (2) continuous monitoring of those devices; and (5) management of corrective actions through ownership and workflow. Used in combination with reactive technoloy such as intrusion detection systems [kap 3.7], proactive network security offers realistic protection by treating threats and vulnerabilities not as isolated events, but as permanent ”features” of the new networked environment”

Detta tänkande skiljer sig från *reactive systems,* så som intrusion detection system. Intrusion detection system är beroende av en attack, incident, eller förlust av data innan informationsuppsamlingen påbörjas och analyseras. Ett *proactive system* testar sitt nätverk kontinuerligt för intrångsmöjligheter. Alla stationer med en IP-adress som är kopplat till nätverket blir ständigt skannade efter profiländringar, brott mot gällande säkerhetspolicy och sårbarhet mot intrång. Efter detta appliceras analys metoder för att ge

administratörerna åtgärdsmöjligheter. Defekten i systemet kan således korrigeras innan det sker ett intrång.

4 Intervjuer

Detta kapitel har för avsikt att ge läsaren en översikt över den input vi har fått från intervjuobjekten.

4.1 *Intervju med Magnus Persson, LDC*

Magnus Persson har arbetet med IT i 23 år. Under denna tid har Persson arbetat som systemerare på Tetra Pak och Securitas. Sedan 1987 har Persson arbetat på Lunds universitet där han började programmera ekonomisystem. Persson har en ADB utbildning avslutad 1980.
Vi började med att fråga Persson vilka brott mot den gällande säkerhetspolicyn som var vanligast vid hans arbetsplats, Persson förklarade,

”Det finns två sorter när man pratar brott mot säkerhetspolicyn. När man medvetet gör något dumt och omedvetet, såsom virus och trojaner. Egentligen är det också ett brott eftersom man måste skydda sin egen dator. Det har man uppenbarligen inte gjort om man inte har patchat dom. Alla datorer som är kopplade mot LUNET ansvarar för sin egen säkerhet vare sig det är privatdatorer eller inte. Alla är ansvariga för sin egen maskin. Se till att den är installerad på ett korrekt sätt så att den inte drabbas. Det som folk medvetet gör oftast är att dom stjäl IP-nummer. 99.9% av dom som stjäl IP-nummer är studenter (användare) som av en eller annan anledning inte kommer ut på nätet. Då provar de ett annat IP-nummer och så krockar det. Då får vi utreda var det är någonstans och stänga den switchporten. Det är det vanligaste.”

Vi undrade då om folk på hans nätverk inte försökte få tillgång till datorer de inte ska ha tillgång till, då svarade Persson,

”Det är ju så att dom flesta inte hackar i eget bo. Våra studenter (användare) är väldigt snälla. Det händer sällan att någon medvetet härifrån hackar. Eller att vi får klagomål i alla fall.”

Frågan gick nu vidare till vilket hot Persson ansåg vara allvarligast inom IT-säkerhet,

”Det beror också på. När det gäller generella hot så är det maskar och trojaner som tar sig in. Där finns det ofta bakdörrar och keyloggers och annat otrevligt som sätter dennes integritet på spel. IT-säkerhetspolicyn på LU är först och främst hot mot liv och person. Det går före datorer. När det gäller data är det som vi är absolut mest rädda för är intrång i LADOK.”

Persson gick nu vidare och berättade om interna risker,

”Det allra största interna riskerna är handhavande problem, alltså att dom som har tillgång till datorerna gör fel. Okunskap, slarv eller tidspress. De finns många orsaker till

varför dom gör fel. Vissa bitar av det är datasäkerhetsproblem andra är inte. Allting är ju ett utbildningsproblem. Den medvetna biten, alltså sabotera medvetet. Det är inget vi har ett större problem med. Men hoten är väldigt stora om en kunnig person verkligen vill göra intrång och har tillgång till maskinerna, datorhallen så att säga. Då har vi stora problem. Men vi har inte haft några sådana tidigare fall av sabotage. Risken att det händer är väldigt låg. Jag vet att man brukar säga att den största risken är intern. Hade det varit så att vi var ett företaget med två brandväggar av olika fabrikat. Då är den största risken intern. Men nu har vi inte så. Nu har vi fritt ut för alla datorer och ingen brandvägg. Då är inte det största hotet internt. När det är säljare som kommer till universitetet här och vill sälja brandväggar och IDS system eller vad det må vara brukar jag säga till dom tänk dig såhär, tänk er hur datasäkerhets sätts upp på ett företag, så tänker du precis tvärtom. Vad är det man gör först? Man sätter upp en brandvägg. Här kan vi inte sätta upp en central brandvägg det finns inte en chans. En brandvägg kan sitta framför en server eller en avdelning. Det finns ingen möjlighet att samsas kring en central brandvägg, det funkar inte. Vi kommer få en 10 gigbits anslutning. Det finns redan GigaSUNET och nu skall vi bygga GigaLUNET. Med ett 10 gigabits backbone. Det finns inte en brandvägg i världen som skulle kunna klara av den trafiken. Ur den synvinkeln är det också ett problem. Att sätta brandvägg framför ett snabbt nät eller övervaka ett snabbt nät är inget som är praktiskt tillämpbart och ingenting som vi har pengar till. Nu när vi bygger GigaLUNET finns en del pengar för att det kommer bli så dyrt ändå, så några 100 000 extra spelar ingen roll. Då kommer vi få in mer saker i nätet. Så att skyddet kommer bli mycket bättre i GigaLUNET. Så att hela byggsatsen passar för övervakning. Det nya nätet kommer ha ny utrustning i switchar och routrar där all trafik kommer passera, om det inte är lokalt i en avdelning. All trafik kommer passera någonstans där vi kan göra en övervakning. Kanske inte insamling av all trafik men så att vi kan upptäcka skadlig trafik från många olika ställen och sammanställa det. Det finns det här Extreme Networks som ni ser här, (Magnus pekar på en anslagstavla med information kring Extreme Networks) vårt nya nät kommer att byggas på deras prylar. I Extreme prylar finns det något som heter clearflow som är ett eget programspråk där man kan berätta att om X antal sekunder ska du cleara, eller plocka ned den i en ickeprioriterad kö och ta ut det på ett övervaknings LAN och spela in trafiken. Man får helt andra möjligheter med ett sådant system.”

Vi ställde nu några frågor om det fanns protokoll som var svårare att säkerställa än andra, Persson svarade,

”Ja det är det i och för sig. När det gäller TCP är det ganska enkelt. Man kan veta vem som tar kontakt med vem. UDP däremot är svårare. Data som skickas vet man inte vad det är, det är ingen som behöver lyssna på det, alltså är det väldigt svårt att se vem som pratar med vem och du kan dölja väldigt mycket i det. Ännu mer besvärligt är det när folk tunnlar information som egentligen ska gå över TCP i IMCP exempelvis. Det finns program för det. Från centralt håll är det ännu svårare att kontrollera ARP protokollet. Om du ska sniffa på ett lokalt nät så måste du göra något som heter ARP spoling, du måste gå in och meddela alla att du ska inte längre prata med default gateway utan du ska prata med mig för jag har övertagit den rollen, då skickas trafiken dit och det görs i ARP spoling. Då syns inte trafiken på det lokala nätet och då kan vi inte övervaka det. Det

enda vi kan se är att alla dessa IP-nummer kommer ut på samma MAC-adress. Vi har ingen möjlighet att ta dom om vi inte gör det under tiden dom skickar trafik.”

Efter lite diskussion om de hackermetoder som omnämnts i kapitel 3.7 frågade vi om någon av dessa är mer relevant än andra.

”Buffer overflows (återfinns i kapitel 3.7), det ligger bakom huvuddelen av attacker idag. De flesta maskar utnyttjar säkerhetshål som bygger på buffer overflow problem. Så det är väl det största. Brut force (omnämns i kapitel 3.7 som password attacks) attacker förekommer också ofta.”

Vi har observerat att området kring IT är dynamiskt och att nya tekniker ständigt utvecklas. Vi bad Persson berätta hur de håller sig uppdaterade,

”Vi brukar, både jag och Alex åka på seminarier i USA. De utbildningar som finns i Sverige och Europa är för dåliga. Vi brukar åka till SANS (www.sans.org) utbildningar. Det är dom som skriver böckerna som lärare lär ut. Vi ligger på olika maillistor också så man vet vad som händer just idag.”

4.2 *Intervju med Björn Ivarsson, SecureIT*

Björn Ivarsson arbetar som IT-konsult på ett företag som heter Secure IT med arbetsuppgifter som inkluderar att evaluera datasäkerhet hos företag och utbildar personal vid implementering av bl a säkerhetspolicies.

På frågan om befintliga hot tycker Ivarsson att hoten som tagits upp tidigare i uppsatsen ger en bra översikt av hotbilden just nu men menar att denna utvecklas och ändras kontinuerligt vilket gör att säkerhetsarbetet måste göra detsamma. Ofta ligger dock utvecklare av virus och liknande steget före. Björn menar att eftersom i stort sett all korrespondens numera ska ske digitalt och ofta via Internet så måste man öka tillgängligheten och därmed ökar hoten och riskerna också. Trots att de yttre hoten ständigt ökar och blir allt mer avancerade menar Björn att det fortfarande är de interna hoten som vållar störst skada. De interna hoten beror på bristande kunskaper och låg medvetenhet hos företagen. Många av de interna hoten skulle försvinna med hjälp av mer utbildning inom informationssäkerhet och mer styrande dokument inom organisationerna. De interna hoten kostar både tid och pengar för företagen. Björn berättar att traditionellt sett lägger företagen större delen av IT-budgeten på tekniska säkerhetsfunktioner istället för utbildning och framtagning av styrande dokument och regler som kan hjälpa till att strukturera upp informationssäkerhetsarbetet och minimera de interna hoten. Vad gäller möjligheter att skydda sig mot hoten anser Björn att man i nuläget, i förebyggande syfte, kan använda sig av befintliga verktyg, exempelvis PAPAI, SBA Check och SBA Scenario. Dessa ger inget fysiskt skydd men han tillägger sedan att det är införstått att företagen har väl fungerande brandväggar och antivirusprogram och andra former av tekniska lösningar då PAPAI och liknande hjälpmedel exempelvis inte skyddar mot intrångsförsök och virusattacker. Däremot tillför de rutiner så att de anställda vet vad de

ska göra för att återställa, efter exempelvis en virusattack. Björn och hans kollegor har under en längre tid använt sig av PAPAI för att säkerställa IT-säkerheten hos kunderna de anlitas av. På senare tid har de även börjat använda sig av SBA scenario för att i ett tidigt skede kunna visa chefer och IT-ansvariga för företagen vad brister i IT-systemet kan kosta företagen, något som SBA Scenario tydligt kan demonstrera. Även om det kan tyckas dyrt för kunden att köra något av scenariona med SBA säger Björn att ofta får detta cheferna att inse att denna kostnaden är obetydlig gentemot kostnaderna som kan uppstå på grund av bristerna som företagen ofta har innan man anlitat IT-säkerhetskonsulter. Vad gäller PAPAI hävdar Ivarsson att detta täcker in det mesta i ett säkerhetsarbete förutom de tekniska analyserna t ex penetrationstest och sårbarhetsanalys och menar att PAPAI mer är ett koncept hur man ska tänka när man arbetar med säkerhet. I verktygslådan finns det checklistor där man kan jämföra vilka krav man uppfyller gentemot t ex ISO 17799 eller BITS. Med hjälp av dessa svar kan man faktiskt även jämföra med andra företag baserat på hur många krav de uppfyllt efter att ha gjort samma test. Riktlinjerna i ISO-standarden ger rekommendationer för ledning av informationssäkerhetsarbetet för säkerhetsansvariga i organisationer. Ivarsson påpekar dock att dessa riktlinjer inte är några krav men bör följas för att uppnå god Informationssäkerhet. Att vara ISO-certifierad på 17799 kan komma att bli en konkurrensfördel inom några år men som det ser ut idag så är det bara ett trettiotal företag som är certifierade i norden. Detta skiljer sig mot andra branscher där företagen har nästintill direkta krav på sig att vara exempelvis certifierade för ISO-standarder för miljö (ISO 14000) och kvalitet (ISO 9000). Krav på företagen inom informationssäkerhet finns inte idag på samma sätt utan i nuläget används ISO 17799 bara som riktlinjer och hjälp för företag att skydda och säkra sina informationstillgångar. I framtiden tror Ivarsson att ISO-kvalitetstandarden kommer gå hand i hand med informationssäkerhetsstandarden 17799 vilket kommer att innebära att fler företag kommer få upp ögonen även för informationssäkerhetsarbetet, vilket i sin tur kommer höja medvetandet hos företagen och i branschen.

4.3 *Intervju med Johan Westlind, TeliaSonera/Portal*

Westlind berättar för oss att han arbetade under ett och ett halvt år som unixtekniker i en av TeliaSoneras serverparker. I denna serverpark fanns runt 300 servrar som ständigt skulle skötas. Westlind berättade att för att säkerställa säkerheten i denna serverpark var den absolut vikigaste uppgiften att ständigt patcha datorerna med säkerhetspatchar. För att hålla sig a jour med tekniker kring säkerhet fick Westlind gå på cirka 3 seminarier angående IT-säkerhet i månaden.

Vi frågade Westlind vad han ansåg det största hotet inom IT-säkerhet, och han svarade,

”Det är svårt att identifiera ett hot som det allvarligaste. Det finns flera saker som är väldigt allvarliga. Det värsta som kan hända är att någon lyckas roota en server (att få administrativa rättigheter). Det finns hundratals sätt att gå till väga för att göra detta. När telia.se blev hackat i slutet av 90-talet berodde det på en samba-share (finns förklarat i kapitel 3 som Shared Library attacks) som hade fel rättigheter så väldigt små missar kan

leda till katastrof. Interna risker är något att se upp med också. Framför allt gäller det svaga lösenord som användare sätter. Det är enkelt att rätta till detta med en password policy som tvingar användarna att använda långa lösenord med blandade siffror och bokstäver samt att de måste byta under vissa tidsintervaller."

Vi bad Westlind att utveckla sitt resonemang kring påståendet om att det fanns så många allvarliga hot.

"Att sända okrypterad data är väldigt allvarligt då det är relativt enkelt att sniffa Internettrafik. Om man inte håller sina applikationer och operativsystem i uppdaterat skick kan man råka ut för attacker (återfinns i kapitel 3 som Application-Layer attacks). När man pratar om säkerhet fastnar man lätt kring det tekniska men man får absolut inte glömma de mänskliga aspekterna som kan göra ett datanätverk sårbart. Detta är social engineering. Människor vill gärna hjälpa till, i sin iver att göra någon till lags kan man ge ut mer information än vad man skall. Det klassiska fallet av social engineering är att en användare blir uppringd av någon som utger sig för att vara nätverkstekniker och ber att få användarens lösenord för att "rätta till ett fel som uppstått". Detta har flera personer försökt med på Telia. Trots att personal blir tillsagd att aldrig lämna ut sina användaruppgifter gör man det ändå. Jag vet inte varför."

Vi bad Johan berättade om några enkla metoder för att skydda sig mot IT-hot.

"I dagsläget ska man fortfarande undvika att köra trådlösa nätverk på arbetsplatser med känslig information, eftersom det tar under en timme att knäcka en WPA nyckel.
Självklart ska man köra en brandvägg där man stänger allt från början och öppnar därefter successivt för dom tjänster som behövs. En uppdaterad antivirusklient på alla datorer i nätverket är också en självklarhet för att avvärja hot.
Även en backup-lösning är ett måste för alla företag, men kan också vara till stor hjälp för privatpersoner som till exempel fått hela sitt fotoalbum raderat."

5 Analys och diskussion

Detta kapitel har för avsikt att genom teori och empiri diskutera vilka IT-hot som är mest väsentliga.

5.1 *Hot som berör omedvetenhet*

Det har framkommit genom teori att omedvetna hot kan ställa till med stora problem. Dessa omedvetna hot förfaller inom skalan för interna hot och återfinns i kapitel 3.2 Olyckor och misstag, 3.3 Insiderproblem samt i 3.7 Malicious Software.

I vår teori nämns olika faktorer som kan bidra till att ett omedvetet hot uppstår

Insiderproblem – Personal som delar med sig av systemet
Ovana användare
Felaktigheter som begås av erfarna användare och systemadministratörer
Nyinstallation av program och uppgraderingar
Införande och test av nya system
Program och utrustning
Olyckshändelser som brand och översvämningar

När det gäller hot som berör omedvetenhet fick vi inte lika mycket stöd ifrån vår empiri som vi fick vid medvetna hot. Magnus Persson på LDC förklarade för oss att det vanligaste brottet inom den gällande säkerhetspolicyn på hans arbetsplats var just brott som användaren gjorde sig skyldig till omedvetet. Främst genom att ha trojaner eller virus på sitt system. Magnus framhöll att de interna hoten ofta var utbildningsproblem. De användare som bryter mot den gällande säkerhetspolicyn har förmodligen inte haft uppsikt över sin dator under en längre tid eller kan vara en ovan användare som inte har kunskap nog att freda sig från dessa program.

Vi fick således lite stöd för de omedvetna hoten som togs upp i vår teori. Vi tror att detta kan bero på att dessa punkter har en nära förankring till åtgärder som berör förebyggande arbete mot IT-hot. Detta kan då medföra att lösningar som används för att arbeta i förebyggande syfte mot IT-hot kan eliminera vissa hot som förfaller inom skaran av omedvetna hot. Vi tänker då på utbildningslösningar och riktlinjer som finns förklarat om PAPAI och ISO-standarden 17799. Dessa kan medföra att många av de omedvetna hoten förfaller. Även om Magnus berättar för oss att det vanligaste brottet på hans arbetsplats är ett omedvetet hot har fokusen av samtalen vi haft med IT-tjänstemännen legat i att arbeta preventivt och på så vis kan man även lösa de omedvetna hoten.

5.2 *Riktade attacker*

I vår teori har vi nämnt några av de vanligaste tillvägagångssätten angripare av system kan använda sig av.

Buffer overflow attacks
Application layer attacks
Shared Library attacks
Social engineering
Password Attacks
Technologial vulnerability attacks
Packet sniffing
Denial-of-Service attacks
IP-spoofing *(kapitel 3.6)*

Detta område skapade mycket diskussion med intervjuobjekten och vi fann mycket stöd till vår teori här.

Björn Ivarsson höll med oss om att de metoder vi har nämnt hör till de vanligaste men upplyste oss om hur snabbt dessa metoder utvecklas och nya tillkommer. Magnus Persson ansåg att Buffer overflows stod för de allra flesta attacker idag. Johan Westlind påpekade att metoden att angripa ett system inte är särskilt relevant då vilken som helst av dessa metoder kan leda till förödande konsekvenser. Johan gav oss ett exempel på detta då han förklarade för oss att en av de allvarligaste intrången hos Telia berodde på något så litet som en samba-share som hade fel rättigheter. Det Johan ansåg som det farligaste hotet var att någon lyckades roota en server. Det tolkar vi som att alla metoder som kan leda till att en maskin rootas anser Johan är allvarligast. Johan upplyste oss också om att man inte fick haka upp sig på de tekniska aspekterna då människor kan falla offer för riktade attacker i form av social engineering. Social engineering finns förklara i kapitel 3.6. Johan berättade för oss om ”det klassiska social engineering försöket” som har försökts på hans arbetsplats. En användare blir uppringd av någon som utger sig för att vara nätverkstekniker och ber att få användarens lösenord för att rätta till ett fel som uppstått. Just detta exempel använde även vi för att förklara begreppet i vår teori. Johan nämnde även lite kort om att svaga lösenord kan göra det lätt för ett intrång att lyckats. Ett intrång som försöker komma åt lösenord kallas password attacks och även detta finns förklarat i kapitel 3.6.

Som de flesta inbrottstjuvar vill även IT-inbrottstjuvar dölja sina spår. Detta område omfattar inte Björns eller Johans arbetsområde då Björn arbetar med preventiva metoder och Johan med serverdrift. Magnus å andra sidan har en roll som liknar en administratör hos en ISP (Internet Service Provider) och kan därav få möta folk på sitt nätverk som vill bryta mot den gällande säkerhetspolicyn och i och med detta sopa igen sina spår. Magnus menade att förövare som använder TCP inte döljer något alls då mottagare och sändare är känt. UDP var däremot svårare att kontrollera då man inte ser vem som kommunicerar med vem och att mycket kunde döljas. Ännu svårare var det enligt Magnus att kontrollera traffik då TCP paket tunnlades genom andra protokoll, exempelvis ICMP. Slutligen

berättade Magnus att övervakning av ARP protokollet var ytterst knepigt. För att övervaka det protokollet var man tvungen att ta över rollen som default gateway och ertappa förövaren under tiden han skickar trafik.

Riktade attacker som togs upp av IT-tjänstemännen.

Buffer overflow attacks – Enligt Magnus Persson den vanligaste

Application layer attacks – Kan enligt Magnus och Johan motverkas genom att ständigt uppdatera sina applikationer och operativsystem.

Shared Library attacks – Metoden som användes för att bryta sig in hos Telia i slutet av 90-talet

Social engineering – En form av attack som riktas mot användarens okunskap, men är samtidigt en riktad attack

Password Attacks – Åtgärdas enligt Johan av en passwordspolicy som tvingar användaren att byta lösenord ofta och använda en kombination av siffror och bokstäver

De punkter som inte togs upp av intervjuobjekten var

Technologial vulnerability attacks
IP-spoofing
Denial-of-Service attacks

Magnus berättade för oss om hur användare på hans nätverk kunde stjäla IP-adresser (*IP-spoofing)* för att få åtkomst till Internet då sin egen är blockerad. Syftet var inte att gömma sin egen identitet eller få åtkomst till specifika IP-block utan att komma runt en blockad som lagts på den egna adressen. Vi tycker inte att det är *IP-spoofing*. *Technologial vulnerability attacks* som involverar en attack på en specifik del av systemet, regelmässigt operativsystemet och inte en applikation som *Application layer attacks* har liknande lösningar såsom patchar. *Denial-of-Service attacks* togs inte heller upp. Anledning till att det inte talades om detta var att ingen hade råkat ut för det men alla intervjuobjekten var medvetna om att detta hot fanns.

5.3 *Mjuk- och hårdvara för att skydda sig mot IT-hot*

Det finns hjälpmedel för att skydda sin verksamhet mot IT-relaterade hot. På Magnus Perssons arbetsplats fanns det för tillfället ingen möjlighet att ha en brandvägg som skyddar hela LUNET. Det beror på att det är för mycket trafik som går igenom och med den utrustning de har finns det ingen brandvägg som klarar av att sköta den trafiken. Magnus berättade för oss om det nya nätet som Lunds Universitet skall kopplas mot, GIGASUNET. För att koppla upp sig mot detta nätverk krävs det att LUNET uppgraderar sitt backbone för att kunna möta den inkommande hastigheten. I och med detta kommer

det göras inköp av utrustning som lättare kan anpassas för att övervaka sin trafik. Extreme Networks står för de mesta av de nya inköpen. All trafik som sänds över Extreme Networks routrar kommer kunnas övervakas med hjälp av ett konfigurationsprogrammeringsspråk som heter clearflow.

Johan Westlind förklarade för oss att han tyckte de var väldigt viktigt att kryptera sin trafik som är känslig. Johan anser att det är mycket enkelt att sniffa trafik och det säkraste sättet att se till att informationen man sänder inte kommer i fel händer är att kryptera den. Vi har förklarat de två vanligaste sätten att kryptera sin trafik.

Symmetrisk kryptering och asymmetrisk kryptering (kapitel 3.9.3)

Johan menade också att patchar till sina applikationer och operativsystem alltid måste vara uppdaterade om man vill undvika intrång.

Vi har i vår teori i kapitel 3.9.4 berättat om IDS (Intrusion detection systems). Ingen av de intervjuade har haft särskilt mycket att säga om just detta. Vi tror att det beror på att deras arbetsuppgifter inte täcker det område där ett IDS används. Magnus har berättat att LUNET inte är gjort för att ha en central brandvägg och/eller IDS. Johans arbetsuppgifter var att se till att servrarna han ansvarade över var i drift och Björn arbetade inte med så tekniskt djupgående uppgifter.

Den försvarsåtgärd som det talas mest om i IT-säkerhetssammanhang är firewalls eller brandväggar (kapitel 3.9.1). Dessa är så självklara att intervjuobjekten inte har valt att prata så mycket om dem. Magnus nätverk lämpade sig inte för en centralbrandvägg och Johan arbetsuppgifter låg innanför brandväggar. Björn menade att det är i princip underförstått att ett nätverk som är kopplat mot Internet har en eller flera brandväggar.

IPSec som förklaras i kapitel 3.9.2 talades det inget alls om med intervjuobjekten. Detta är ett system som kan användas istället för kryptering (som har diskuterats) då kryptering är en del av programvaran.

5.4 *Verktyg för att arbeta i förbyggande syfte mot IT-hot*

Både teori och input från de olika intervjuerna har visat att utbudet på verktyg som ska skydda informationssäkerheten i förebyggande syfte är begränsat. Vi har i kapitel 3.10 i teorin beskrivit de tre olika verktygen vi lyckats identifiera; SBA Check, SBA Scenario och PAPAI samt ISO-standarden 17799. Varken Johans eller Magnus arbetsuppgifter var sådana att de behövde befatta sig med verktyg av det här slaget, vilket troligtvis förklarar varför deras kännedom kring dessa var liten. Däremot kunde Björn utveckla dessa tre verktygen som vi tagit upp i teorin och förklara dessa mer ingående för oss eftersom hans arbetsuppgifter är just sådana och han arbetar dagligen med två av dessa; SBA Scenario och PAPAI, vilka han också föredrar framför SBA Check, som arbetar med hjälp av olika checklistor och hjälper organisationen leva upp till övergripande krav. Dessa olika verktyg ger inget fysiskt skydd men Björn tillägger att det är införstått att företagen har

väl fungerande brandväggar och antivirusprogram och andra former av tekniska lösningar. Han nämner att det största och det enligt honom mest användbara verktyget av dessa är PAPAI. Vi nämnde i teorin (kapitel 3.10.4) att

”Syftet med PAPAI-konceptet är att ge ett praktiskt stöd och ett färdigt ramverk för säkerhetsarbetet. Metoden åskådliggörs grafiskt på ett antal webbsidor som uppdateras under arbetets gång och bildar ett processorienterat ledningssystem för informationssäkerhet. Till detta hör ett stort antal mallar, checklistor, projektaktiviteter mm. Dessa används som utgångspunkt i det egna säkerhetsarbetet och gör det möjligt att snabbt ta fram egna policies, riktlinjer och annan dokumentation som också läggs in i den färdiga PAPAI-strukturen.”

PAPAI är alltså ingen tekniskt applikation utan snarare vad Björn beskriver som ett koncept hur man ska tänka när man arbetar med informationssäkerhet. PAPAI, som står för: Policy, Analys, Plan, Arkitektur och Planering är ett ledningssystem för informationssäkerhet. PAPAI och liknande hjälpmedel exempelvis skyddar inte mot intrångsförsök och virusattacker, däremot tillför de rutiner så att de anställda vet vad de ska göra för att återställa, efter exempelvis en virusattack. PAPAI är, enligt Ivarsson, det mest heltäckande verktyget där man, i olika steg, går från verksamhetens krav hela vägen ner till den slutliga implementeringen. Under arbetet med PAPAI arbetar man med samtliga inblandade i organisationen vilket är bra på så sätt att alla anställda då får klarhet i vad som krävs och tillåts för att god informationssäkerhet ska uppnås. Man arbetar alltså hela vägen från ledningsnivå och administrativ nivå ända ner till den tekniska nivån. En fördel med PAPAI är att verktyget är uppdelat i olika paket vilket gör att företag och organisationer själv kan bestämma vilka man vill köpa in beroende på hur pass mycket känslig information man känner att man har och till vilken grad denna behöver skyddas.

På senare tid har de på företaget Secure IT även fått mer och mer användning av SBA Scenario som på ett tydligt sätt visar för kunderna vilka konsekvenser för företagets resurser brister i det befintliga IT-säkerhetssystemet kan få. Trots att vi i teorin nämnde att SBA Scenario är ett dyrt verktyg så visar det sig ofta att kostnaden för införskaffandet av detta verktyg är nästintill försumbar jämfört med vad en katastrof orsakad av dålig informationssäkerhet hos ett företag kan vara.

I teorin har även ISO-standarden 17799 tagits upp. Denna är inte ett verktyg på samma sätt som de tre tidigare nämnda är, men ändå viktig att förklara eftersom denna och andra standarder såsom BITS ofta används i de olika verktygen för att jämföra och se vilka krav kunden uppfyller gentemot dessa. Att vara ISO-certifierad på 17799 kan komma att bli en konkurrensfördel inom några år enligt Björn, som även tillägger att direkta krav på företagen inom informationssäkerhet inte finns idag utan i nuläget används ISO 17799 bara som riktlinjer och hjälp för företag att skydda och säkra sina informationstillgångar.

6 Slutsatser

Efter att ha studerat teori och input från intervjuobjekten har vi funnit vissa IT-hot som anses vara allvarliga än andra. Vi har även funnit möjligheter att skydda sig mot IT-hot.

De allvarligaste hoten har vi identifierat i vår teori och empiri och är

Insiderproblem

Ovana användare

Program och utrustning

Olyckshändelser som brand och översvämningar

Buffer overflow attacks

Application layer attacks

Shared Library attacks

Social engineering

Password Attacks

Anledningen till varför vi valt dessa hot som de allvarligaste är att varje punkt som nämns kan bidra till att en dator ”rootas”. Vilket innebär att förövaren vid ett lyckat intrång kommer åt administrationsrättigheter. Undantaget här är *Olyckshändelser som brand och översvämningar.*

De möjligheter att skydda sig mot IT-hot som vi funnit i vår teori och empiri utöver de självklara som brandväggar, IDS och antivirusprogram är

PAPAI

SBA Scenario

Utrustning som gör övervakning av nätverket möjligt

Uppdaterade (patchade) applikationer och operativsystem

Utbildade användare

Vi har valt PAPAI pga. av den struktur den tillför en organisations IT-miljö. Vid användandet av PAPAI har man skyddat sig mot hot såsom *Password Attacks* och *Olyckshändelser som brand och översvämningar* i och med att man har en Password-policy och ett back-up system. Problem med ovana kan också motverkas då ett nytt säkerhetstänkande har förankrats i organisationen från ledningen till gräsrotsnivå. De anställda har då blivit införstådda i vilka rutiner som gäller. Det kan gälla mycket enkla rutiner såsom de regler som gäller vid inkommandet av e-post som innehåller bilagor. Insiderproblem är alltid svårt att skydda sig mot. Policys, regler och behörigheter kan tillsammans med en teknisk implementation av skyddsåtgärder hjälpa till att förhindra dessa hot. Beträffande social engineering hjälper även PAPAI till med att implementera rutiner som gäller besök hos organisationen. Vanligtvis har företaget egna regler för detta men det finns även med i PAPAI. Det gäller rutiner som loggning av besökare efter uppvisad legitimation samt att mottagaren på företaget får komma ned personligen och hämta besökaren. Därefter förses besökaren med en besöksbricka.

SBA Scenario finns att använda som ett test för att se vilka konsekvenser bristerna i sin IT-miljö kan få. Det är således mycket användbart när man skall evaluera sin IT-säkerhet och för att se vilka områden som kan behöva bättre säkerhetslösningar. Man kan även få ut en kostnadsanalys för att se vilka ekonomiska kostnader bristerna kan medföra.

De två tekniska punkterna vi har valt som innebär möjligheter att skydda sig mot IT-hot har vi valt pga av deras egenskaper i säkerhetssammanhang. Uppdaterade applikationer och operativsystem är det mest givande sättet att se till att *Buffer overflow attacks, Application layer attacks* och *Shared Library attacks* inte är användbara intrångsmetoder. Att utrustningen man använder gör det möjligt att övervaka sitt nät innebär att man kan implementera system som IDS och brandväggar vilket är väldigt viktiga komponenter inom IT-säkerhet.

Den sistnämnda punkten eliminerar de onödigaste av IT-hot. Att någon av ovetskap förlorar data eller öppnar upp möjligheter för intrång.

Genom att vara väl införstådd i dessa aspekter som berör IT-hot tror vi att man kan underminera chanserna av att ett intrång sker på sitt nätverk och om ett intrång sker rädda så mycket data som möjligt. Man skall dock vara vaksam över vad alla intervjuobjekten var eniga om, att utvecklingen av metoder för att göra intrång ligger före utvecklingen av metoder för att motverka intrång.

7 Källförteckning

7.1 *Publicerade källor*

Bell, Robert, Impure science: fraud, compromise, and political influence in scientific research (1992)

Pleeger, Charles P.: “Security in computing”, Prentice-Hall, 1997-2000, ISBN: 0-13-337496-6.

SOU 2004:32; ”Informationssäkerhet i Sverige och internationellt – en översikt”, 2004, ISBN: 91-38-22108-X.

Stallings, William: ”Network Security Essentials – Applications and Standards”, Prentice Hall, 2003, ISBN: 0-13-120271-5.

Gurley Bace, Rebecca: “Intrusion Detection”, Macmillan Technical Publishing, 2000, ISBN: 1-57870-185-6.

Ewert, Magnus: “Datakommunikation”, Studentlitteratur, 2001, ISBN: 91-44-01735-9.

Svensson, Anders: ”Analyzing Information System Security”, Paper accepted for publishing, Department of Informatics, Lund 2005.

Panko, Raymond R.: ”Business Data Networks and Telecommunications – Fourth edition ” Natalie E. Andersson, 2003, ISBN: 0-13-048727-9

Post och Telestyrelsen, Rapport, PTS-ER-2005:15

Samhällets säkerhet och beredskap, regerings prop. 2001/02:158

Material från Björn Ivarsson, Secure IT i samband med intervju

William Buchanan: ”Mastering Networks”, Macmillan, 1999, ISBN: 0-333-69343-4

Cisco Systems: Internetworking Technology Overview. Security Technologies, 1999

Tim Keanini: ”Proactive Network Security: Making Your Network Unassaible” Information Systems Security: Mar/Apr 2005; 14, 1

7.2 *Muntliga källor*

Björn Ivarsson, IT-säkerhetskonsult Secure IT, ”Diskussion kring IT-säkerhet”, intervju av Marcus Holmquist och Oscar Stibeck, 13/05/05.

Magnus Persson, Datasäkerhetssamordnare LDC, medlem i Lunds Universitets IT-säkerhetsgrupp, ”Diskussion kring IT-säkerhet”, intervju av Marcus Holmquist och Oscar Stibeck, 18/05/05.

Johan Westlind, Unixadministratör TeliaSonera och senare hos Portal, ”Diskussion kring IT-säkerhet”, intervju av Marcus Holmquist och Oscar Stibeck, 08/05/05.

7.3 *Elektroniska källor*

Länk 1
Wikipedia,
http://en.wikipedia.org/wiki/Buffer_overflow

Länk 2
Nationalencyklopedin,
http://www.ne.se/jsp/search/article.jsp?i_art_id=713287&i_word=trojanska%20h%e4star&i_h_text=1&i_rphr=trojanska%20h%e4star

Länk 3
Symantec,
http://www.symantec.com/region/se/corporate/sakerhetsskola_virus_maskar_trojaner.html

Länk 4
The ISO 17799 Directory,
http://www.iso17799software.com/

Länk 5
IDG, Skapa ramverk för IT-säkerhetsarbetet, Hans Husman
http://arkiv.idg.se/transfer/?aid=13990

Länk 6
PAPAI,
http://www.papai.se/

Länk 7
Secure-IT,
http://www.secure-it.se