Institutionen för informatik och matematik

Informationssäkerhet

En undersökning om säkerhetsarbetet bland företag i Dals-Ed.

Information security
An investigation in security management among companies in Dals-Ed.

Uppsats fördjupningsnivå 1 i
Informatik
10 poäng
Examinationsversion 2003-11-10

Examinator: Lars Svensson
Handledare: Gunnar Peterson
Författare:
Bengtsson, Jenny
Olsson, Jenny

Sammanfattning

Dagens snabba tekniska utveckling har bidragit till stora förändringar för många företag, från att lagra all information på papper till att i möjligaste mån sköta all dokumentation på datorer och lagra information i informationssystem. I takt med denna utveckling har även utvecklingen för att kunna skada informationen gått, om inte snabbare. Det är därför viktigt att företagen inser vikten av att skydda sin information. Som utgångsläge för vår uppsats har vi antagit hypotesen att företag i Dals-Ed inte har insett allvaret med att skydda sig. Syftet är därmed att undersöka medvetenheten bland dessa företag om hoten mot informationssystemen. För att genomföra vår studie har vi använt oss av både en kvantitativ och en kvalitativ undersökning. Detta har resulterat i att ge oss en inblick i hur säkerhetsarbetet fungerar hos företagen. För att kunna bygga upp ett bra skydd för sin information måste företagen känna till de hot som finns. Efter 11 september, 2001 har säkerhetsmedvetenheten ökat mer och mer runt om i världen. Trots detta är säkerhetstänkandet enligt flera källor bedrövligt på många företag. En oerhört viktig del i uppbyggnaden av säkerhetsarbetet i företagen är säkerhetspolicyn. Det är dessa riktlinjer som medarbetarna bör arbeta efter. För att kunna skapa en sådan policy måste dock en riskanalys och ett hotscenario göras. Vår kvantitativa undersökning omfattade cirka 30 företag varav ungefär 15 svarade. Enkätundersökningen visade på att hälften av företagen hade en säkerhetspolicy. Det visade sig också att i större delen av företagen hade inte alla anställda tillgång till Internet då det skulle öka riskerna. Andra uppgifter som framkom var att enda säkerhetsåtgärden hos en del företag som hade uppkoppling mot Internet var antivirusprogram. När vi studerade resultaten från den kvalitativa undersökningen som omfattade intervjuer med tio företag visade det sig att det var ett fåtal av dessa som hade någon form av policy. Det var dessutom en Internet- och e-postpolicy, ingen omfattande säkerhetspolicy. Även i den kvalitativa undersökningen såg vi dock tendenser av att företag med Internetuppkoppling saknade något vidare skydd mot hoten än antivirusprogram. Men det framkom också att en del företag har ett mycket omfattande säkerhetsarbete trots att de saknar en dokumenterad säkerhetspolicy. Vår slutsats är att vi inte funnit tillräcklig information som visar på att vår hypotes är sann. Dock kan vi påstå att säkerhetsarbetet inte ligger på en godtagbar nivå bland vissa företag i Dals-Ed. En intressant vinkel på en fortsatt studie skulle vara en jämförelse av säkerhetstänkandet mellan företag i en tätort och företag i glesbygd.

Abstract

The technical development is moving extremely fast which contributes to changes for many companies. They have moved from being dependent on papers into using advanced information systems for storing data. With the technical development the growth rate of another development has also increased. That is the knowledge possessed by all the people out there that wants to abuse your information. Therefore the companies must understand the importance of protecting their information. Our starting point for the examination is the hypothesis that companies in Dals-Ed has not realised the seriousness in protecting themselves. The purpose of this paper is to examine the awareness of the threats against information systems among these companies. We have made one quantitative and one qualitative investigation to implement our study. This gave us an insight in the companies' information security management. To be able to build a good security system for the information the companies must know about what kinds of threats there are. After September eleven, 2001 the awareness about information security management has increased more and more around the world. According to several sources the security management is, despite this insufficient in many companies. An extremely important part in the security management in the company is to devise a safety policy. It's these guidelines all the co-workers should work for. To be able to devise a safety policy, a risk analysis and a threat scenario must be carried out. Our quantitative investigation comprises 30 companies of which approximately fifteen answered. The result of the questionnaire showed that about half the companies had a safety policy. We could also see that in most of the companies all the employed didn't have access to the Internet, when this would increase the risks. Other information that came to light was that the only safety measure in some companies that had Internet was an antivirusprogram. When we studied the results of the qualitative investigation that comprised interviews with ten companies, it showed that it was only a few of them that had any kind of a safety policy. Moreover it was an Internet- and e-mail policy, no further safety policy. Also in the qualitative investigation we could see tendencies that companies with Internet lack more safety measures than an antivirusprogram. Information that comes to light is that some companies have an extensive security management even though there is a lack of a documented safety policy. Our conclusion is that we haven't found enough information that proves our hypothesis right, but we can say that the security management doesn't hold an acceptable level among some companies in Dals-Ed. An interesting angle of a future study would be a comparison between the security management of a company in a sparsely populated area and of a company in a heavily populated area.

Innehåll

1. Inledning

Att skydda information är inte något nytt påfund som kommit med tekniken. Behovet att på något sätt sända och överföra information fanns redan långt innan dagens tekniker utvecklades och med det även ett behov av att skydda information. Under de gamla grekernas tid t.ex. rakades huvudet på budbäraren och meddelandet skrevs in. Innan budbäraren fick ge sig av och leverera meddelandet skulle håret ha växt ut (Esser & Svenjeby, 2003). Det som har förändrats är att informationen idag till största delen är digital och att nya tekniker för att skydda den finns tillgängliga. I takt med dagens snabba tekniska utveckling och företagens behov av tillgänglighet gentemot sina kunder, ökar hoten mot informationen som företagen tillhandahåller. Det är viktigt för företagen att kunna förse behöriga med information på ett säkert sätt. Dagens nätverk och en snabbt föränderlig hotbild gör detta till ett mer och mer utmanande uppdrag för varje dag. Ett stort problem i många organisationer är inte nonchalans mot riskerna utan snarare en låg medvetenhet om hoten utifrån. Hoten är indelade i fysiska, logiska samt organisatoriska och det är för det mesta den mänskliga faktorn som är orsaken till att problem uppstår i systemet. Möjligtvis inte alltid avsiktligt utan ibland pga. brist på kunskap(Symantec, 2003).

Hoten mot nätverken blir alltmer avancerade och använder sig av flera metoder för att hitta sårbarheter. Det finns flera sorters hot men det som är oerhört aktuellt idag och som kan orsaka allvarliga problem är olika typer av virus och dataintrång. På senare år har flera ”virusepidemier” härjat på Internet och företag har drabbats hårt där det har kostat miljontals kronor att återuppbygga systemen. Ett exempel på en kostsam återuppbyggnad är annars när USA drabbades av terroristdådet 11 september, 2001 då inte bara människoliv släcktes utan ett flertal företags informationssystem förintades. Detta visar hur sårbart ett företag idag kan vara om inte säkerheten tas på allvar. Att säkerhetsmedvetenheten efter denna händelse ökar mer och mer är ett faktum och den kommer förhoppningsvis att utbreda sig till att omfatta hela världen. Frågan är hur långt har varningarna nått och har allvaret i dem gått fram till företagen? Det kan tänkas att företagen i en glesbygd har uppfattningen att de lever i en skyddad värld och därför inte tar till sig varningarna. Åtminstone inte på samma sätt som företag i stora städer där konkurrensen är större och därmed är rädslan att hemlig information ska läcka ut mer påtaglig. Vi vill påstå att det finns en mentalitet i större delen av Sverige att människor i glesbebyggda områden är godtrogna och naiva i tron att de är ”isolerade”. Därför finner vi det intressant att fördjupa oss i olika säkerhetsmetoder för att kunna undersöka om detta gäller företag belägna i Dals-Ed.

Vi behandlar i uppsatsen vad de olika typerna av hot innebär och vad som bör göras för att förebygga dessa. Det handlar om problemen med bristande säkerhet i informationshantering där vi vill belysa vikten för företagen att vidtaga åtgärder mot hoten. De hot vi kommer att beskriva är de fysiska, logiska samt organisatoriska och vi kommer att koncentrera oss på vilka säkerhetsåtgärder som är aktuella. För att få en bild av varför dessa åtgärder är aktuella tänker vi förklara hur de fungerar och hur de arbetar för att stoppa hoten.

1.1 Bakgrund

I vår uppsats har vi valt att definiera medvetenheten om säkerhetsarbetet i olika kategorinivåer. Dessa nivåer har varit svåra att bestämma eftersom företag har så olika förutsättningar och påverkas på skilda sätt av ett attentat. Exempelvis kan ett företag förlora 100 000 kronor om deras system står stilla i två dagar medan ett annat förlorar 10 gånger mer på bara några timmar. För att kunna ge läsaren en tydligare bild av säkerhetsarbetet har vi

försökt generalisera företagen efter deras sårbarheter och skydd. Vi har nedan definierat kategorinivåerna låg, medel och hög medvetenhet.

Låg medvetenhet
Företag med Internetuppkoppling som saknar säkerhetsåtgärder eller endast har ett antivirusprogram och data- och strömbackuper. Företaget saknar helt säkerhetspolicy eller använder sig inte av den.

Medel medvetenhet
Företag med Internetuppkoppling som vidtagit grundläggande säkerhetsåtgärder vilka är antivirusprogram, brandvägg, data- och strömbackuper och helst intrångsdetekteringssystem. Antivirusprogrammet bör uppdateras minst en gång om dagen. Företaget har en säkerhetspolicy som delvis är implementerad i företaget där anställda får ta del av den.

Hög medvetenhet
Företag med Internetuppkoppling som vidtagit åtgärder utöver ”medel”. Företaget arbetar kontinuerligt för att utveckla sitt säkerhetsarbete och håller sig uppdaterat på nyheter. De har även en väl genomarbetad säkerhetspolicy som är anpassad efter företagets verksamhet och där analys om hoten och riskerna gjorts. Det bör ingå en krisplan i säkerhetspolicyn.

2. Syfte

Syftet med uppsatsen är att undersöka säkerhetstänkandet hos företag i Dals-Ed om de är medvetna om hoten mot informationssystemen. Genom att granska företagens säkerhetsarbete vill vi antingen finna stöd eller motargument till vår hypotes.

Vi förväntar oss att vårt arbete ska tillföra oss kunskap och insikt i hur utsatt informationen i företagen är och varför säkerhetsarbetet är en viktig del i organisationens arbete. Vi eftersträvar även kunskap om hur säkerhetsåtgärderna fungerar. Dessutom vill vi bidra till en ökning av medvetenheten hos företagen om de externa hoten för att minska risken att drabbas.

2.1 Problemformulering

Vi har ställt oss följande frågeställning vid utgångspunkten för vårt arbete:
- Är företag i Dals-Ed medvetna om de risker som uppstår då organisationens information hanteras och lagras på datoriserade informationssystem?
- Har de någon säkerhetspolicy?
- Vilka hot finns och vilka åtgärder har företaget vidtagit?

Med denna frågeställning som grund har vi kommit fram till en hypotes som vi utgår från under våra fortsatta studier.
”Företag i Dals-Eds kommun har låg medvetenhet angående säkerhetsarbetet kring informationshantering.”

2.2 Avgränsningar

Genom ett samarbete med ÅF - Ångpanneföreningen som är ett IT-företag i Dals-Ed har vi fått tillgång till information från dem och möjlighet att genomföra intervjuer med företag i deras närområde om säkerhetstänkandet. Därför är vårt arbete avgränsat till företag lokaliserade i Dals-Ed.

Informationssäkerhet är ett väldigt brett ämne som omfattar skydd mot flera olika typer av hot och vi har därför valt att begränsa oss till det som för oss känns väldigt aktuellt idag. Detta är vilket vi tidigare nämnt, hoten mot informationssystemen som på olika sätt kan skada företagens lagrade information. Vi väljer att koncentrera oss på hur företagen skyddar sig, dvs. vilka tekniker de använder sig av och hur väl personalen på företaget är insatt i informationshantering. Vi behandlar de vanligaste hoten och hur funktionerna hos de olika metoderna och teknikerna för ökad säkerhet ser ut.

3. Metod

Metoddelen sägs utgöra en av de tre viktigaste delarna i en uppsatsskrivning. Tillsammans med problem- och resultatdelen utgör de ”skelettet” i den vetenskapliga uppsatsen. Anledningen till att skriva en detaljerad redovisning av metoden är dels evaluering och dels replikation. Det sistnämnda innebär att det ska vara möjligt för någon annan under identiska förhållanden att utföra metoden för att kontrollera resultatet. Det förstnämnda är en värdering och undersökning av bärkraften av metodik och problemställning, för att se om slutsatser och tolkningar är korrekta (Backman, 1998).

Ett sätt att utföra sin forskning på är att genom enkäter, undersökningar av statistik, mätningar etc. komma fram till ett resultat i form av numeriska observationer eller sådana som låter sig översättas till det. Detta kallas för ett kvantitativt förhållningssätt. En kvalitativ undersökning resulterar inte i siffror eller mätbar statistik utan ger en helhetsbild av problemet som ställts upp. Resultatet är formuleringar som kan vara skrivna eller uttalade (Backman, 1998).

Vi har valt att göra en kvalitativ undersökning där vi genomförde tio intervjuer. Anledningen till detta är för att komma företagen närmare och få en djupare inblick i hur säkerhetsarbetet fungerar i verkligheten. Respondenterna är dessutom mer öppna och villiga att tala om sina säkerhetslösningar då vi möter dem ansikte mot ansikte. Intervjumallen som vi använde oss av är delvis semistrukturerad och delvis riktat öppen med frågeområden där respondenten fördjupar sig i det som intervjuaren finner meningsfullt (Lantz, 1993). Vi valde även att utforma den med en låg grad av standardisering där ordningsföljden inte är bestämd utan bestäms av respondenten. Detta för att inte låsa respondenten vid frågorna så att information som eventuellt kan vara till nytta kan komma fram (Trost, 1997).

Vissa delar av teorin kan förefalla något teknisk men pga. att en del av personerna vi skulle intervjua arbetar med informationssäkerhet och teknik hela dagarna ville vi kunna ta del av informationen och veta vilka följdfrågor som skulle vara relevanta. Detta innebär att vissa delar i teoriavsnittet endast har som syfte att öka förståelsen.

Under arbetets gång har vi till viss del tagit hjälp av den hermeneutiska metoden vilket innebär att bearbetning av text och undersökningar ger en successivt ökande inblick och förståelse för området. Det brukar kallas att en typ av texttolkning utförs och i detta fall även tolkning av intervjuer. Det kan också uttryckas som så att ”den hermeneutiska metoden innebär ett systematiskt tillvägagångssätt för sökandet efter inre mening och helhetsförståelse” (Befring, 1994, s.82). Det är viktigt att vi är medvetna om att vi tolkar utifrån vissa premisser pga. tidigare erfarenheter. Tanken är att försöka förstå att det vi tolkar är en del av en helhet vilken säkerhetsarbetet ingår i. Med detta menar vi att säkerheten som vi undersöker i företaget endast är en del i hela verksamheten och att det måste tas hänsyn till det (Befring, 1994).

Vi har även använt oss av ett hypotetisktdeduktivt förhållningssätt där utgångspunkten är en teori vilken det härleds hypoteser ur som styr forskningsprocessen och framarbetningen av enkäter och intervjumall. Redan innan vi började skriva kände vi oss nyfikna på att undersöka medvetenheten om säkerhet hos olika företag och då vi upplevde att människor i glesbygden på ogrundad fakta får kritik att de är oförsiktiga ville vi undersöka om så är fallet i Dals-Ed. Vi anser därför att det var en intressant hypotes vi arbetade fram. Motsvarigheten till ett hypotetisktdeduktivt förhållningssätt är ett hypotetisktinduktivt förhållningssätt där observationer och analyser av fenomen leder fram till hypoteser och eventuella nya teorier (Befring, 1994).

Reliabilitet, tillförlitligheten och validitet, giltigheten i uppsatsen är två viktiga saker som bör granskas. Det vill säga, skulle någon annan kunna göra om uppsatsförfattarnas undersökning och komma fram till samma resultat, respektive mäter undersökningen det som den avsetts att mäta? Detta bör ifrågasättas just för att se om forskningen kan tillföra vetenskapen något eller om det bara är att kasta slutsatserna i papperskorgen (Strömquist, 1999). Dessa variabler är dock endast intressanta att undersöka och granska då en kvantitativ undersökning har gjorts. Eftersom delar av vår forskning har varit kvantitativ kommer vi att utvärdera reliabilitet och validitet endast i delar av uppsatsen (Eneroth, 1984).

I vår uppsats anser vi att reliabiliteten inte är så hög eftersom vi har en svarsfrekvens på enkäten med endast 42 %. Anledningen till detta kan vara flera orsaker. Vi valde att sända ut enkäten till företag som hade e-postadress via bifogad bilaga med e-post för att det skulle gå snabbt och lätt för företagen att svara. Företagen kan ha ansett att det innebar en risk för virusattentat att öppna den bifogade filen och bestämt sig för att det var bäst att inte öppna bilagan. Detta problem försökte vi komma runt genom att erbjuda dem som fick enkäten via e-post att istället få den skickad till sig via post om de föredrog det. Vi skickade även ut en påminnelse tre veckor senare vilket gjorde att vi fick in några enkäter till. Att endast hälften av företagen som fått enkäten svarat gör att slutsatser vi dragit från den kvantitativa analysen bör användas något försiktigt.

Validiteten däremot anser vi är relativt hög. Frågorna på enkäten är enkla, korta och har krävt endast en kort stunds insats för att besvara. Frågorna var även av sådan karaktär att den IT-ansvarige bör veta svaren utan att behöva fråga någon annan eller leta efter svaren i dokumenterade papper. Därmed anser vi att enkäten ger oss en grund som visar på hur företagens säkerhetsarbete är utformat vilket är det vi vill mäta. Tyvärr är det alltid en viss risk att frågorna har misstolkats och att frågorna på något sätt upplevs som kränkande så att respondenten inte vill svara helt sanningsenligt. De kan känna sig fördummade för att de inte har vidtagit åtgärder som det frågas om i enkäten etc.

I arbetet med den kvantitativa delen hade vi kunnat använda oss utav den deskriptivtanalytiska metoden men eftersom den oftast används vid stora datamängder och då svaren refererar till både många personer och många variabler anser vi inte att den passar in i vår undersökning. Metoden tillämpas dessutom ofta då det undersökta stickprovet är komplicerat och oöversiktligt. Vanligtvis är det nödvändigt med en forskningsinsats för att få kunskap om de samband som gäller, vilket vi inte tycker stämmer överens med vår undersökning (Befring, 1994).

Tillvägagångssätt
Vi valde att utföra en delvis kvantitativ och kvalitativ undersökning. Detta för att få mer information och vara säkrare på de slutsatser som vi eventuellt skulle komma fram till.

Förutom intervjuer sökte vi information i böcker men även bland artiklar i aktuella tidningar och på Internet. Detta för att erhålla den senaste teknikens framsteg och för att kunna hålla uppsatsen ajour. För att ge de slutsatser vi dragit större trovärdighet läste vi in oss i tidigare studier om säkerhetsarbetet bland företag.

Vi började undersöka företagen med hjälp av en enkätundersökning som vi utformade tillsammans med vår handledare och vår uppdragsgivare. Denna enkät skickades ut till alla företag i Dals-Eds kommun som fanns med på Företags Faktas hemsida med fem anställda eller fler. Detta resulterade i 33 företag varav tolv stycken fick enkäten med post och de resterande fick den via e-post. Vi gav dem möjlighet att svara med e-post, vanlig post eller fax (Se bilaga 1).

Urvalet till intervjuerna skedde på så sätt att vi valde ut fem stycken företag av vår uppdragsgivares kunder och fem stycken företag som inte är deras kunder. Vi försökte även i möjligaste mån välja så stora företag som möjligt eftersom vi trodde att de skulle ha en mer utvecklad IT-miljö. Även dessa frågor arbetade vi fram tillsammans med handledare och uppdragsgivare (Se bilaga 2). Intervjuerna genomförde vi tillsammans samtidigt som vi bandade dem. De genomfördes på respektive företag och tog ungefär 25-30 minuter. Vi försökte gå ut till företagen utan att låta oss påverkas av våra tidigare studier i ämnet. Dvs. vi ville ha samma inställning till alla företag och inte förutsätta att något företag skulle ha sämre säkerhetsarbete än något annat. Anledningen till det var att vi inte ville att vår inställning skulle påverka resultatet av intervjuerna. Resultatet bearbetade vi sedan på så sätt att vi lyssnade av banden minst två gånger och tog ytterligare anteckningar för att komplettera de från intervjutillfället. Pga. att bandspelaren vi lånade vid högskolan var trasig kunde endast delar av intervjuerna bandas. Detta medförde att vi inte kunde skriva ut hela intervjuerna ord för ord.

För att ingen utomstående ska kunna skada något av dessa företag pga. den information vi lämnar ut, har vi valt att respondenterna ska få förbli anonyma. I enkätsvaren är t.o.m. en del av respondenterna anonyma för oss som skribenter.

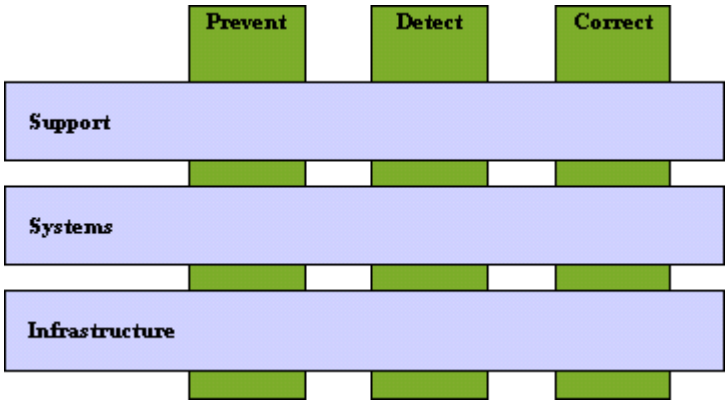
Felkällor

För att kunna göra en grundläggande bedömning av resultatet i vår undersökning bör frågor som ”Är stickprovet representativt för populationen” och ”Hur stort är bortfallet” besvaras (Eriksson & Wiedersheim, 2001). Eftersom vi valt att undersöka hela populationen i Dals-Eds kommun pratar vi inte längre om ett stickprov inom kommunen utan en undersökning där Dals-Ed representerar ett stickprov ur företag i glesbygd i Sverige. Pga. bortfallet kan vi inte säga att vår undersökning representerar hela populationen, dvs. Dals-Eds kommun. Trots påminnelser från vår sida har inte alla företag svarat. Varför de företag som ingick i undersökningen inte har svarat är svårt att besvara men det bör dock diskuteras om det kan finnas någon systematisk orsak till att dessa företag har handlat som de gjort eller om det bara beror på ointresse. Det kan tänkas att dessa företag har en så dålig säkerhetshantering av informationen på företaget att de inte vill besvara enkäten för att de tycker att den är förolämpande. Vi angav att de kunde vara anonyma men eftersom det är svårt att vara anonym på Internet ger det kanske en känsla av avslöjande. För att få en bild av bortfallet hade vi kunnat välja ut några av dessa företag och se till att vi fick in svar från dessa. Men vi nöjde oss med att dra slutsatsen att företagen saknar intresse att delta i vår undersökning. Detta pga. att de företag som svarade efter påminnelsen inte skiljde sig från de övriga.

Källkritik
När vi sökte information gjorde vi det på flera ställen för att på så sätt kunna värdera den fakta vi använt oss av. Vi har försökt välja källor som ger trovärdig information men vi är dock medvetna om att viss fakta inte alltid är helt objektiv. Eftersom informationssäkerhet är ett ytterst aktuellt ämne idag och många organisationer som arbetar med att utveckla skydd mot hoten lever på detta kan det hända att dessa källor överdriver vikten av säkerheten. Då vi upplever hoten som så pass omfattande och därför finner det viktigt för företagen att skydda sig har vi ändå valt att använda oss av denna information. Vi vill dessutom att vår uppsats ska vara ajour med utvecklingen och värderar informationen från dessa källor utefter deras kunskaper om tekniken. Eftersom vi anser att de har de senaste teknikerna och kunskaperna vill vi ta del av detta.

4. Informationssäkerhet

Informationen är en av de mest värdefulla tillgångarna ett företag har, trots att det är en ganska abstrakt tillgång. Då det är en värdefull tillgång är det viktigt att implementera skydd för att öka säkerheten mot riskerna med att lagra digital information. Det är detta som informationssäkerhet handlar om. Det gäller att vid användandet av informationsteknologi försäkra sig om att IT-hanteringen sker på ett lämpligt sätt. IT-hantering eller på engelska IT-management handlar om att välja rätt standarder, modeller och lösningar i takt med den snabba och komplexa tekniska utvecklingen. Säkerheten definieras som så att det är att upprätthålla sekretessen, tillgängligheten och integriteten hos informationen. Det omfattar både digital och ickedigital information samt att mildra eventuella händelser. Säkerheten relaterar också till riskhantering som handlar om att alla risker bör ges ett värde som motsvarar vad de resulterar i finansiella förluster då de uppstår. Det finns processer för både IT-hantering och informationssäkerhet att förlita sig på vid driften av IT-miljön (Se figur 1) (Wallhoff, 2002).



Figur 1 Stödjande processer vid informationssäkerhet och IT-hantering. (Wallhoff, 2002)

Nyckeldelarna i IT-miljön är processerna infrastruktur, system och hjälp (support). Infrastrukturprocessen innefattar servrar, nätverkstopologi och operativsystem. Detta är den viktigaste delen för att kunna implementera och upprätthålla en organisations IT-plattform. Processen system handlar om alla system och databaser som stöder de processer organisationen är beroende av. Ovanför dessa ligger hjälpprocessen som rör aktiviteter så som övervakning och helpdesk, men även definiering och utvärdering av IT-strategin. Säkerhetsprocesserna kan definieras till att förebygga (prevent), upptäcka (detect) och korrigera (correct) att/om/när händelser uppstår. De kan baseras på tekniska lösningar men människor måste uppmärksammas på riskerna. Processen förebygga handlar om att försvåra

för en händelse att uppstå, upptäcktsprocessen är hur organisationen inser att de drabbats och korrigeringsprocessen innebär hur organisationen ska återuppbygga skadorna för att ta sig tillbaka till utgångsläget igen. Detta kan vara en grundläggande hjälp vid utvecklingen av en säkerhetspolicy (Wallhoff, 2002).

Den 12 september 2002 skrivs det en artikel i tidningen Nerikes Allehanda om en undersökning där det framkom att över 50 % av de svenska storföretagen satsade miljarder på IT-säkerhet och katastrofskydd efter terrorattackerna mot USA den 11 september 2001 (Nerikes Allehanda, 2002). Skadorna efter 11 september blev bestående, det var inte bara den stora förlusten av människor utan med de två tornen försvann också hela företag och deras informationssystem. Då IT-säkerheten var bristfällig blev det en omöjlig uppgift att återskapa program och kunskap lagrat i företagens datorer. Detta hårda uppvaknande har lett till stora investeringar i IT-säkerhet. I hela världen ökar säkerhetsmedvetandet. Det svenska dataföretaget Veritas har, enligt tidningen i en undersökning omfattande ett 50-tal svenska storföretag ställt frågor angående IT-säkerhet. 85 % av de tillfrågade företagen har en plan för oväntade IT-avbrott, investeringarna i IT-säkerhet har ökat hos över 40 % av företagen varav 60 % uppger 11 september som orsaken. Frågan är då: Gäller detta även företag i glesbygd? IT-säkerhetsmedvetandet ökar runt om i världen, därmed även Sverige. Men hur långt har det nått? Är företag belägna i glesbebyggda områden införstådda med att det föreligger hot även mot deras information? Enligt Jonas Ahlberg, ansvarig för Jonas webresurs är säkerhetstänkandet på företag i allmänhet bedrövligt. De anställda beter sig oerhört riskfyllt genom att bl.a. ladda ner filer och spel på företagets datorer, öppnar misstänkta dokument som kommit via e-post etc. Varje år uppskattas kostnaderna för att reparera sådant till många miljoner. Han anser att företagen inte ger sina anställda nödvändig information eller datorutbildning. Det händer att inte ens cheferna vet hur säkerhetstänkandet bör fungera. Idag har användarna väldigt lite kännedom om verktygen de använder och när något går fel kallas teknikerna dit. För att öka säkerheten i organisationer måste samarbetet mellan säkerhetsmedvetna personer och användarna öka och på så sätt sprida informationen i företagen (Ahlberg, 2003).

4.1 Hoten

För att kunna skapa en fungerande säkerhet i organisationen måste företaget känna till de hot de är utsatta för och de svagheter de har. Det är kännedomen om dessa som möjliggör ett väsentligt säkerhetsarbete i företaget. Hur skyddar ett företag sig mot något som de inte vet att de behöver skydda sig mot? Det är därför viktigt att göra företagen medvetna om vilka hot som finns därute (Andersson, 1999).

Organisatoriska hot

”Det räcker inte med produkter eller konsulter. Företaget måste också jobba på rätt sätt.” Detta är orden som skrivs på förstasidan på Computer Swedens extrabilaga TEMA Säkerhet fredagen den 5 september 2003. För att skydda sig mot intrång och virus räcker det inte med den senaste tekniken och säkerhetsutrustningen för i slutändan sitter användaren ändå där och kan förstöra en hel sköld mot virus bara genom att göra några ogenomtänkta val. För att komma på rätsida med detta problem, som är ett organisatoriskt hot mot företaget, gäller det att hålla sina anställda uppdaterade om hur de bör agera i olika situationer.

De vanligaste orsakerna till att detta problem uppstår är en otydlig organisation med bristande roll- och ansvarsfördelning. Denna fördelning bör skrivas ner i en säkerhetspolicy där rollerna finns inom organisationen för att se till att policyn efterlevs. För att det ska fungera i praktiken

måste alla få utbildning inom sitt område och fullt ut förstå vilka uppgifter och vilket ansvar som föreligger på varje roll (Mitrovic´, 2001). Vikten av roller kommenterar även Staffan Jackson på Ekelöw Infosecurity. Alla anställda behöver inte utbildas i detalj vad gäller IT-säkerhet men alla bör veta vem de ska vända sig till med frågor (Danielsson, 2003). Staffan ger även tre grundläggande tips:

- Alla måste veta vem de ska prata med om säkerhetsfrågor
- Bygg in säkerhetsrutiner i det dagliga arbetet
- Skriv ner instruktioner för hur system ska tas i drift på ett säkert sätt

Företaget behöver även en väl utvecklad behörighetsadministration som är en mycket viktig funktion för att tilldela eller ta bort rättigheter till IT-resurser. När en ny person blir anställd på företaget bör denna få en egen identitet vilket oftast sker genom ett anställningsnummer. Därefter bör personen förses med rättigheter till adekvata IT-resurser för att kunna sköta sina arbetsuppgifter. Om en person slutar ska tillgången till IT-resurserna blockeras eller tas bort. Detta underlättar tillgängligheten, integriteten och sekretessen i IT-resurserna. Tyvärr är det så att personal och medarbetare ibland kan ha motiv att ta sig in på obehöriga sidor vilket gör denna administrativa del så viktig. Dessa intrång är mycket svårare att skydda sig emot än de intrång som kommer utifrån (Mitrovic´, 2001).

Logiska hot

Under denna rubrik finner vi de hot som på något vis är kopplade till programvaran i IT-systemen. Det kan vara operativsystem, tillämpningar, databaser och liknande. Det finns olika typer av logiska hot och vi kommer här att förklara de vanligaste. En typ av logiskt hot är när någon obehörig loggar in sig på någon annans konto i systemet. Beroende på vilka rättigheter som har tilldelats det användarkontot kan den obehöriga personen orsaka allvarlig skada i tillgängligheten, integriteten och sekretessen i IT-resursen.

Systemattacker har de senaste åren drabbat stora handelsplatser t.ex. www.yahoo.com eller www.amazon.com. Denna typ av attack har förhindrat tillgängligheten i systemen. Legitima användare har förnekats utföra sina ärenden. Exempel på en sådan attack är DoS-attacker vilket betyder Denial of Service. Det antagligen mest kända logiska hotet som har slagit ut med full kraft inte minst det senaste året är virus och säkerhetshål i Microsofts operativsystem. Varningstexterna haglar över oss samt vilka åtgärder som bör vidtagas för att skydda sig. Det är främst virus-, mask- och trojanangrepp men kombinationer är också mycket vanliga. Dessa kan ställa till med mer eller mindre systemskada om det tar sig in och kan t.o.m. lamslå en hel fabrik under flera dagar. Detta kostar enorma resurser varpå företag i dagsläget är noga med bandbackuper ifall något skulle hända (Fjordvang, 2002).

En virusattack beskriver ibland lite generellt alla typer av attacker från elak programkod som kan attackera våra datorer. Här får vi en översikt över hur de olika typerna av virus arbetar.

- Virus – Ett virus är en snutt programkod som har till uppgift att sprida sig och föröka sig. Viruset kan inte göra någonting om det inte finns i ett program, script eller kommandofil. När ett virus utvecklas läggs det därför i ett program med slutbokstäverna .com eller .exe. Viruset kan även läggas i kommandofiler som har slutbokstäverna .bat eller .pif. En kommandofil består av en uppsättning kommandon som kan sätta igång en process i ditt operativsystem som börjar radera filer. Scriptfiler har slutbokstäver som .vbs (Microsoft Visual Basic) eller .js (JavaScript source code). Dessa typer av filer återfinns särskilt i samband med webbläsaren. Dessa script är

farliga pga. att de kan aktivera andra program via din webbläsare eller genom att fungera som egentliga program (Fjordvang, 2002).

- Mask – Maskar är självständiga program som har till enda uppgift att föröka sig. Den ändrar ingenting utan bara fyller minnet på datorn med en massa kopior av sig själv (Esser & Svenjeby, 2003).

- Trojansk häst – Är ett eget program som finns i anslutning till ett vanligt program som användaren själv installerar på sin dator. Det kan vara ett spel eller liknande. När väl programmet har börjat användas kan trojanen börjar utföra sina instruktioner i bakgrunden av det program som användaren installerat. Detta program kan inte kopiera sig själv vidare vilket gör att det är helt beroende av att användaren delar med sig av sitt nya program (Fjordvang, 2002).

Fysiska hot

Det är det enklaste hotet att definiera. Det är skador på allt synligt som t.ex. hårddiskar, kretskort, moderkort, skärmar, skrivare etc. Det kan vara allt från brand till inbrott, översvämning till sabotage. Om någon av dessa incidenter skulle inträffa är det inte mycket det går att göra åt materialen, men informationen som finns lagrad går att rädda med grundläggande och kontinuerliga säkerhetsrutiner. Finns det rutiner som att bandbackuper körs varje natt och det en natt skulle börja brinna har endast den sista dagens arbete gått förlorat. Vad som inte bör glömmas bort är att bandbackuperna bör helst förvaras på annan adress än servern eftersom de flesta brandsäkra skåp håller temperaturen nere på en tillräckligt låg nivå för att banden inte ska ta skada endast några timmar (Mitrovic´, 2001).

4.2 Åtgärder

GM marknadskommunikation har gjort en undersökning omfattande över 800 små och medelstora företag i Norden som visar att många saknar grundläggande säkerhetsskydd. Det är därför oerhört stor risk att de drabbas av cyberattacker som GM uttrycker det. Mindre än hälften av företagen hade en brandvägg installerad och 20 % saknar helt antivirusskydd. Det är då inte förvånande att 27 % av företagen uppger att de någon gång förlorat information eller att systemen legat nere pga. intrång eller virusinfektioner. I 47 % av företagen ligger säkerhetskompetensen under medel medan 37 % säger att de har kontroll över säkerheten i sina system. När det gäller IT-säkerhetspolicy var resultatet ungefär femtio-femtio. Trots det var det 64 % som uppgav att de inte hade någon krisplan för att snabbt och effektivt kunna hantera en säkerhetsincident (Symantec, 2003).

En grundläggande sten i uppbyggnaden av säkerhetsarbetet i en organisation är säkerhetspolicyn, där en krisplan bör ingå. Säkerhetspolicyn ska vara de riktlinjer som alla medarbetare arbetar efter. Den underlättar dessutom företagets val av tekniska säkerhetslösningar såsom brandväggar, kryptering osv. (Dimension, 2003).

Joakim von Braun, säkerhetsrådgivare på Symantec säger:

”Att vara uppkopplad mot Internet betyder att du med största sannolikhet kommer att komma i kontakt med elak kod, hackare och annat bus på Internet. Det är oroande att en så stor del av de nordiska småföretagarna inte verkar vara förberedda på att hantera virus, trojaner, maskar, hackare och andra vanliga former av cyberattacker. Våra rekommendationer är att företag

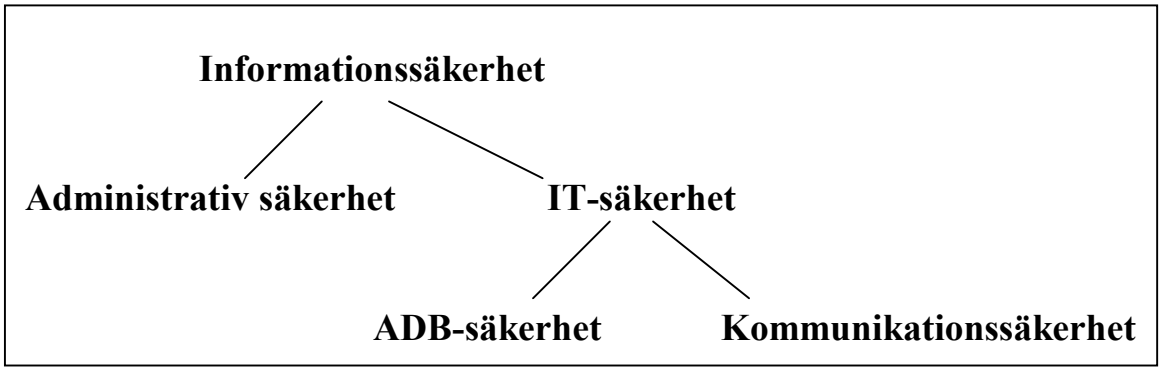
åtminstone installerar antivirus och en brandvägg – och helst intrångsdetektering också." (Symantec, 2003).

Joakims fem tips till småföretagare

- Enbart antivirus räcker inte. Att skapa total säkerhet går inte men en brandvägg och IDS (Intrångs Detekterings System) förbättrar klart dina chanser. Idag finns integrerade lösningar med alla dessa funktioner på marknaden.
- Utveckla en säkerhetspolicy och kommunicera den till de anställda.
- Sök information om säkerhet från fler än en källa: prata med återförsäljare, IT-säkerhetsleverantörer, eller externa IT konsulter. Läs IT-press och besök webbsajter om säkerhet.
- Uppdatera, uppdatera, uppdatera. Installera patchar så snart de blir tillgängliga – vänta inte på en sårbarhet.
- Om säkerhetshanteringen blir för tidskrävande och tar för mycket resurser från din kärnverksamhet, fundera på att lägga ut driften av säkerheten på en specialist som kan hantera din säkerhetsmiljö.

4.3 ADB-säkerhet och kommunikationssäkerhet

Informationssäkerhet kan skapas i två huvuddelar där det ena är administrativ säkerhet som handlar om hantering av information i en traditionell pappersmiljö. Medan det andra är IT-säkerhet, dvs. säkerhet kring informationen som finns lagrad i informationssystem. Säkerhetstänkandet handlar i båda fallen om att skydda informationen när den hanteras på olika sätt och när den lagras för framtida användning. Det är IT-säkerheten som är av intresse för oss och denna kan också delas upp i två grupper, nämligen ADB-säkerhet och kommunikationssäkerhet (Se figur 2) (Andersson, 1999).



Figur 2 Informationssäkerhet (Andersson, 1999)

ADB-säkerhet

ADB-säkerheten innebär skydd av information och datasystem mot obehörig åtkomst och oavsiktlig skada vid behandling av informationen. ADB (automatisk databehandling) är mestadels hantering av information som utförs med datorer. Det omfattar även persondatorer, ordbehandlare och andra maskiner som lagrar och bearbetar information. ADB-säkerhet delas ofta in i tre underavdelningar:

- Konfidentialitet: Skydd mot att obehöriga kommer åt informationen.

- Tillgänglighet: Ser till att en behörig person kommer åt det data den vill komma åt.
- Integritet: Skyddar informationen så att den inte ändrats (Arnesjö, 2000).

Kommunikationssäkerhet
Kommunikationssäkerheten är säkerhet vid överföring av information. National Computer Security Association (NCSA) har identifierat fyra huvudpunkter för säkra transaktioner.

- Autenticitet: Garanterar att den som sänder är den han/hon utger sig för att vara.
- Sekretess: Skyddar innehållet så att bara sändaren och mottagaren känner till det.
- Integritet: Skyddar meddelandet så att det varken medvetet eller omedvetet ändras under transaktionen.
- Icke förnekande: En sändare kan inte förneka att han/hon sänt ett meddelande samt mottagaren kan inte förneka att han/hon tagit emot ett meddelande (Westerlund & Åström, 2001).

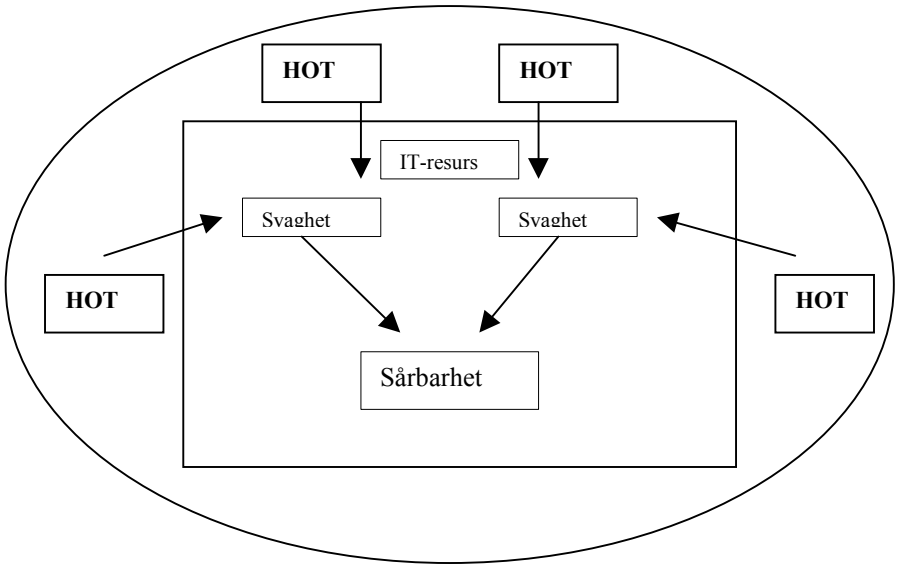
4.4 Säkerhetspolicy

Säkerheten på arbetsplatsen måste genomsyra hela arbetet men för att börja någonstans måste vissa regler och mål dokumenteras i en säkerhetspolicy på företaget. Mitrovic´ definierar säkerhetspolicy så här:

> ”Formellt fastställd uppsättning mål som beskriver övergripande säkerhetskrav på informationshanteringen inom en organisation eller verksamhet.” (Mitrovic´, 2001, s.24).

Denna blir användbar i arbetet mot de fysiska, logiska och organisatoriska hoten som finns. För att utveckla en övergripande säkerhetspolicy kan det vara bra att göra en riskanalys och ett hotscenario (Mitrovic´, 2001).

Riskanalys och hotscenario
När ett hotscenario, som är en viktig del i säkerhetspolicyn, ska utvecklas gäller det att se över alla IT-resurser som organisationen har tillgång till och basera det på olika hotbilder som föreligger. Försök identifiera vem som tjänar på att bryta sig in i systemet. Tänk dig sedan in i personens situation. Måla upp riktiga och verklighetsförankrade hotscenarier och koppla riskerna till varje scenario om det skulle inträffa. Riskanalys sker genom att identifiera riskerna och uppskatta sannolikheten för att de inträffar. Hur stora blir kostnaderna och vilka blir konsekvenserna om något skulle inträffa? För att åskådliggöra strukturerandet av hoten se figur 3.



Figur 3 Hotbild (Mitrovic´, 2001)

Hot är någon form av handlingar eller händelser som kan skada organisationens IT-resurser. Dela in hoten likt tidigare beskrivning i fysiska, logiska och organisatoriska hot. Svagheter är eventuellt kända eller okända brister i IT-resursernas tekniska utformning. Även bristande beredskap i form av dålig rutin, organisation, administration och intern kontroll (kvalitetssäkring) hör till denna grupp. Sårbarheten är hur utsatt en IT-resurs är genom sannolika hot och kända svagheter.

Detta arbete kan leda fram till ett beslutsunderlag som motiverar kostnaderna för att investera i IT-säkerhet i form av mera personal och mer utrustning. Att förvalta en säkerhetspolicy är inte enbart IT-avdelningens uppgift utan istället är det ett övergripande ledningsansvar. För att utveckla en bra säkerhetspolicy behövs ingående instruktioner som vi inte kan återge här men vi rekommenderar boken Handbok i IT-säkerhet, (Mitrovic´, 2001) där författaren går igenom steg för steg vad som bör planeras och utföras.

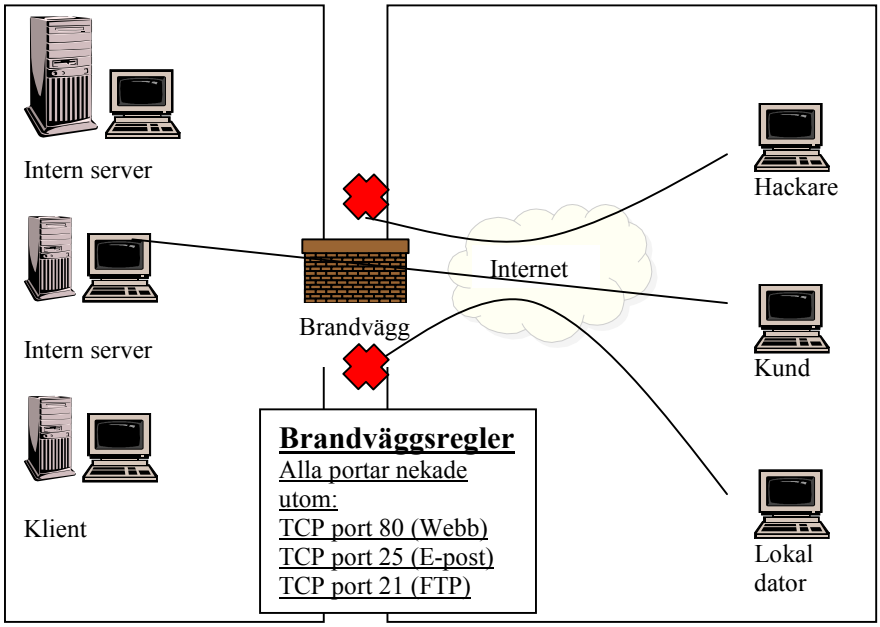
4.5 Brandväggar

En brandvägg i ett hus har som funktion att hindra att bränder sprider sig mellan hus. Det vill säga den isolerar husen från varandra. Detta kan jämföras med att isolera nätverk från varandra för att inte få in oönskade saker. Det vanligaste är att isolera det interna nätverket mot Internet. En brandvägg har två extrema lägen; helt stängd eller helt öppen. Om brandväggen står i något av dessa lägen är den i stort sett onödig. Är den helt stängd är den väldigt säker men det finns inga dörrar eller fönster i den så varken trafik ut eller in är tillåten. Är den däremot helt öppen tillåts all sorts trafik vilket gör att säkerhetsnivån blir minimal. Brandväggen ska därför öppnas bara precis så mycket som är nödvändigt, vilket ger optimal säkerhet. Det är dock viktigt att skilja på högsta möjliga säkerhet och optimal säkerhet då högsta möjliga säkerhet innebär att brandväggen är helt stängd (Oppliger, 2000).

Syftet med en brandvägg är att kontrollera åtkomsten mellan ett säkert nät och ett mindre säkert nät. Den skyddar interna nät mot attacker från Internet. Det förutsätts då att alla hot som riktas mot informationen i det interna nätet kommer från Internet, vilket inte alltid är sant. En brandvägg kan därför användas för att kontrollera trafik åt båda hållen. Om en dator kommer åt Internet kan alla på Internet komma åt datorn men genom att installera en brandvägg är det enbart denna som är ansluten till Internet. All säkerhet ligger då på ett ställe,

i brandväggen. Kommunikationen sker via brandväggen och där kan regler sättas upp för hur kommunikationen får se ut (Safeit, 2003).

Brandväggar används inte bara mellan interna nät och Internet utan även mellan olika interna nät, mellan Internet och servicenät och mellan interna nät och servicenät. Ett servicenät är ett nät där tjänster läggs som allmänheten ska komma åt. T.ex. möjligheten att surfa till en hemsida eller skicka och hämta filer. En brandvägg ger också möjligheten till att logga allt som händer mellan Internet och det interna nätet. Det vill säga arbetsgivaren kan övervaka och kontrollera allt som görs. Med en brandvägg centraliseras alla säkerhetstjänster i maskiner som är avsedda för uppgiften och på så sätt minimeras tiden som behövs för att ansluta, verifiera och kryptera data i höghastighetsnät (Atremo, 2003) (Se figur 4).



Figur 4 En brandvägg spärrar oönskad trafik. (Strebe & Perkins, 2002) Omgjord.

Komponenter i brandväggen

Brandväggar använder i huvudsak följande tre grundläggande metoder:

- **Paketfiltrering**: Paketfilter är gränsroutrar som genom att kontrollera om ett paket ska skickas vidare eller inte ökar säkerheten. Kontrollerna görs genom informationen som finns i paketens huvud (Gääw & Lindström, 2001).
- **Network Address Translation** (NAT): Med hjälp av NAT kan problemet med att dölja interna datorer på TCP/IP-nivå lösas. Det ser ut som att all trafik kommer från en och samma IP-adress, nämligen brandväggens (Almgren & Johansson, 2003).
- **Proxytjänster**: En mellanserver som används för att kontrollera och godkänna transaktioner mellan användaren och värddatorn. En proxy kan styra vad som ska vidarebefordras förbi en brandvägg (Pagina, 2003).

4.6 Intrångsdetekteringssystem (IDS)

Intrångsdetektering innebär identifikation av digital eller elektronisk aktivitet som är elakartad eller otillåten. Genom att söka igenom innehåll och uppträdande hos Internettrafik, för att leta efter elak kod eller attacker adderar ett intrångsdetekteringssystem ett extra lager av säkerhet. Systemet körs hela tiden i bakgrunden och övervakar all trafik som rör sig ut och in i datorn. Systemet letar efter trafik som är misstänksam, onormal eller som överrensstämmer med ett känt hot. Då IDS upptäcker en misstänkt aktivitet varnas användaren eller så agerar IDS enligt inställningar som användaren gjort. För att få bästa resultat bör användaren själv konfigurera nivå och vilken typ av aktivitet som ses som elak och sedan ställa upp olika policys för hur dessa beteenden ska behandlas. Precis som ett inbrottslarm övervakar misstänkt aktivitet runt ditt hus, varnar IDS säkerhetsadministratören om möjliga hål i nätverket (Symantec, 2003).

4.7 Kryptering

Krypteringstekniken utvecklades för att dölja information från obehöriga. Information som överförs över t.ex. Internet är speciellt utsatt och det är därför av stort intresse att dölja denna information på bästa sätt. Det kan också användas till att identifiera vem som kommunicerar med vem genom att skapa en digital signatur. Tekniken ger även möjligheten att kontrollera att dokumentet inte förändrats. Grunden i kryptografi är ett kodsystem som används. Det finns flera olika metoder för kryptografi och för varje metod finns olika sätt att räkna, så kallade algoritmer. Ju mer komplicerad och svårgenomtränglig metoden är desto mer tid tar det för datorn som krypterar (PKI-Forum, 2003).

Symmetrisk kryptering använder samma nyckel för kryptering som för dekryptering. Det vill säga att både sändare och mottagare har samma nyckel. Symmetrisk kryptering är ofta aktuell i situationer som kräver hög hastighet. Formeln är inte så komplicerad vilket underlättar för datorn. Asymmetrisk kryptering däremot använder sig av två olika nycklar, en privat och en publik. Kryptering med den ena nyckeln kan endast dekrypteras med den andra. Det som styr valet av metod är behovet av säkerhet och snabbhet (Ficora, 2003).

4.8 VPN – Virtuella Privata Nätverk

När man använder Internet för att koppla ihop lokala nätverk uppstår problem gällande säkerhet, prestanda, pålitlighet och underhåll. Det beror på att datorer långt borta ges möjligheten att koppla in sig på nätverket. För att göra det så svårt som möjligt för hackare att komma åt privat information har de flesta brandväggar i ett företag konfigurerats för att inte släppa igenom tjänsteprotokoll som NetBios, NetWare Core Protocol eller NFS. Skulle dessa protokoll däremot vara tillåtna att släppas igenom kan anställda komma åt fil- och utskriftstjänster utifrån, men detta innebär att även hackare kommer åt dessa data. Det lokala nätverket blir på så sätt inte privat. Lösningen på detta problem är VPN – Virtual Private Network (Strebe & Perkins, 2002).

Genom kapsling av LAN-trafiken i IP-paket används Internet för att routa trafiken från ett privat nätverk till ett annat. Dessa paket är krypterade och därmed oläsbara för mellanliggande Internetdatorer. VPN kan skapas genom att använda serverdatorer, brandväggar eller routrar. IP-kapsling innebär att ett IP-paket innehåller ett annat IP-paket. Det kan göra att det för nätverksdatorer ser ut som om två avlägsna nätverk är nära varandra och skilda åt genom en enda router. Detta trots att de är åtskilda av många Internetroutrar och gateways som kanske inte ens använder samma adressområde eftersom NAT används (Oppliger, 2000).

För att säkert bestämma identiteten för en fjärranvändare och på så sätt besluta vilken grad av säkerhet som är rätt används kryptografisk autentisering. VPN använder sig av det för att se om användaren kan vara delaktig i den hemliga tunneln och genom autentiseringen utbyts den hemliga eller publika nyckeln som används vid kryptering av last. I sin tur används kryptering av datalast för att dölja innehållet i inkapslad data(Strebe & Perkins, 2002).

4.9 Virusskydd

Förr spred sig virus enbart via disketter medan dagens virus sprider sig med e-post, HTTP, exekverbara filer och ett flertal andra metoder. Att skydda företag mot virus är en av nätverksadministratörens svåraste uppgifter. För att underlätta arbetet för företagen arbetar virusföretagen ständigt med att hitta nya och bättre metoder för att stoppa virusen innan de hinner exekvera (Svidén, 2003).

Magnus Carling skriver att antalet virus som idag existerar är svårt att uppskatta men det handlar om mellan 70 000 och 80 000 varav ungefär 400 aktivt sprids vid varje tänkbart tillfälle. Varje månad uppkommer det cirka 800 nya virus! Tillverkarna av antivirusprogram har alltså fullt upp med att skydda sina kunder, mot både nya och gamla virus. Detta görs på flera olika metoder. Den vanligaste och äldsta av dessa metoder är att skanna filer och matcha dem mot virusdefinitioner. Virusdefinitionerna lagras i en signaturfil och definieras genom den unika kod som viruset består av. Så länge signaturfilen är väl uppdaterad fungerar detta bra men problem uppstår då viruset inte finns i filen. Ytterligare en metod är heuristisk sökning, vilket innebär en identifikation av skadliga beteenden hos exekverande filer. Antivirusprogrammet undersöker då vad ett misstänkt program gör, exempelvis om det gör massutskick via e-post. Risken finns att en sådan skanning stoppar ofarliga program med virusliknande beteenden. Ibland kan ett antivirusprogram dock istället för att stoppa program skicka filerna till antivirusleverantören (Carling, 2003).

Problemet med att skanna efter nya virus är att det tar tid att arbeta fram en ny signaturfil. Som bäst är en ny signaturfil ute inom två till tre timmar efter virusupptäckten. Detta är lång tid när det gäller dagens avancerade virus. Det som tar tid är analysering av virus, inskrivning i signaturfilen, klassificering av virus, testning och tryckning av signaturfilen. Ett nytt virus kan upptäckas på flera olika sätt. Dels kan antivirusprodukterna själva ställas in att rapportera om misstänkta filer och dels skickar administratörer över hela världen in filer de misstänker. När antivirusprogrammen tillåts upptäcka virus själva undersöker även de, beteenden för att upptäcka avvikelser. Sedan en tid finns en policystyrd metod hos de stora antivirusföretagen som stoppar virus baserat på dess namn eller form. Det är ett fåtal av antivirusprogrammen som distribuerar en sådan här policy centralt. En policy kan finnas hos användarna inom 45 minuter från det att ett virus upptäckts (Carling, 2003).

Framtiden

Det senaste för att hitta virus är de policykontrollerande metoderna och förutom dessa finns det inte så mycket nya metoder. Fortfarande är signaturfilerna det mest effektiva sättet att identifiera virusen och hitta åtgärder. Nackdelen med detta är att uppdatering av signaturfiler alltid ligger lite efter virusmakarna som bara utvecklas mer och mer. De virus som är oerhört framgångsrika är kombinationsvirusen, dvs. att de exempelvis är mask och trojan på samma gång. Det är framför allt mot dessa virus som antivirusföretagen lägger ner mycket tid på att uppdatera signaturfilerna. En ökning av dessa virus är att vänta och än så länge är antivirusföretagen väl förberedda. Oron inför framtiden är arkitekturerna som delar applikationer på ett flertal plattformar med olika virusskydd. PDA-plattformarna (Personal

Digital Assistant) är de plattformar som kommer vara särskilt utsatta i framtiden. Det finns redan idag skydd för de vanligaste PDA: erna på marknaden. Instant messagingsystem och ICQ uppfyller också kriterierna för att sprida virus. Samarbetet mellan antivirusföretagen och operativsystemtillverkarna ökar och det finns redan funktioner integrerade i operativsystem för att stoppa virus. Ett exempel är Outlook som har funktioner för att hindra användaren från att öppna exekverbara filer istället för att spara dem lokalt. Lagstiftarna kan också bidra till minskad virusspridning genom att ställa virustillverkarna tillsvars med stränga straff (Carling, 2003).

En bild ur verkligheten
Någonstans ute på den engelska landsbygden ligger Symantecs hemliga virusbunker. Här skannas det dygnet runt efter misstänkta attacker och de upptäcker 10-15 nya virus varje dag. Det är nog inte en slump att SOC – Security Operation Center ligger i ett gammalt skyddsrum med metertjocka väggar, fönsterlösa rum och generatorer som förser anläggningen med ström i 90 dagar vid ett strömavbrott. Allt handlar ju om säkerhet. Här är syftet att upptäcka alla säkerhetshot på Internet så att de företag som köper tjänsterna får snabba varningar. Arbetet kan indelas i två delar – en övervakningsdel och en åtgärdsdel. En analytiker klarar att övervaka 200-250 av kundernas maskiner samtidigt. Information samlas in och läggs i en databas, detta ger analytikern en bild av vad som händer. De ser attacker m.m. och analyserar sedan resultatet för att ge kunderna förslag på vad de måste göra. På en månad fick de in 9,5 miljoner informationsstycken bara från en kund och av dessa hittades 1,3 miljoner möjliga händelser. Av de fastställdes 347 attacker varav 3 stycken var så allvarliga att åtgärd krävdes (Svidén, 2003).

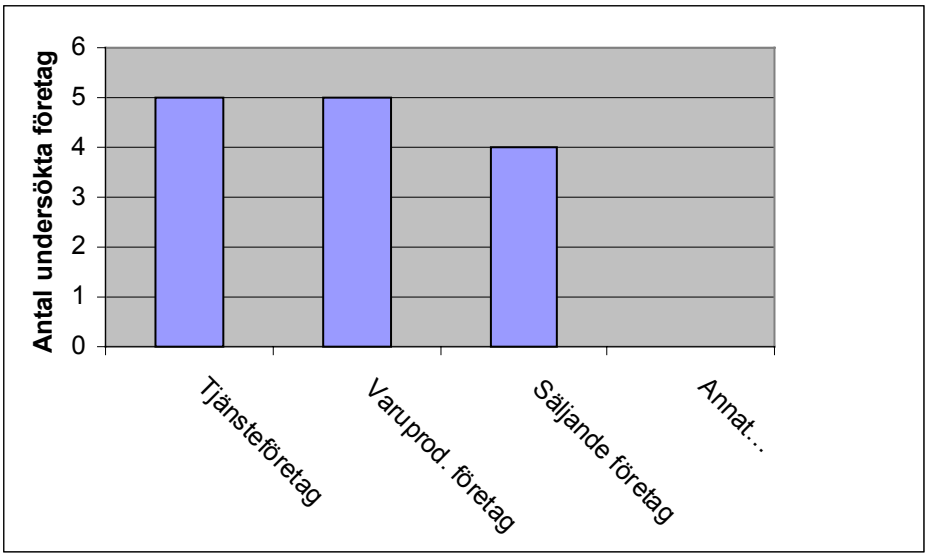
I hela världen är det 122 personer inblandade i arbetet och 16 stycken av dem sitter i Dublin där de ansvarar för Europa, Mellanöstern och Afrika. Det är i Dublin det avgörs om ett virus är farligt, varningar på Symantecs webbplats uppdateras och det arbetas fram uppdateringar som krävs mot viruset (Svidén, 2003).

5. Våra undersökningar

5.1 Enkätundersökning

I vår kvantitativa undersökning valde vi att skicka ut en enkät till alla företag med fem anställda eller fler i Dals-Eds kommun som fanns registrerade på Företags Faktas hemsida 2003-09-10. Vi har en svarsfrekvens på 42 % vilket ger ett bortfall på 19 företag. Detta höga antal svarsbortfall kan ge en sned bild av populationen men vi har ändå valt att presentera den informationen som vi har fått fram. Vi kommer att presentera resultatet på frågorna 1, 2, 7, 13, 15 (se bifogad enkät) i olika typer av tabeller och diagram. Eventuella kommentarer som vi har fått på dessa frågor står publicerade nedan i löptext.

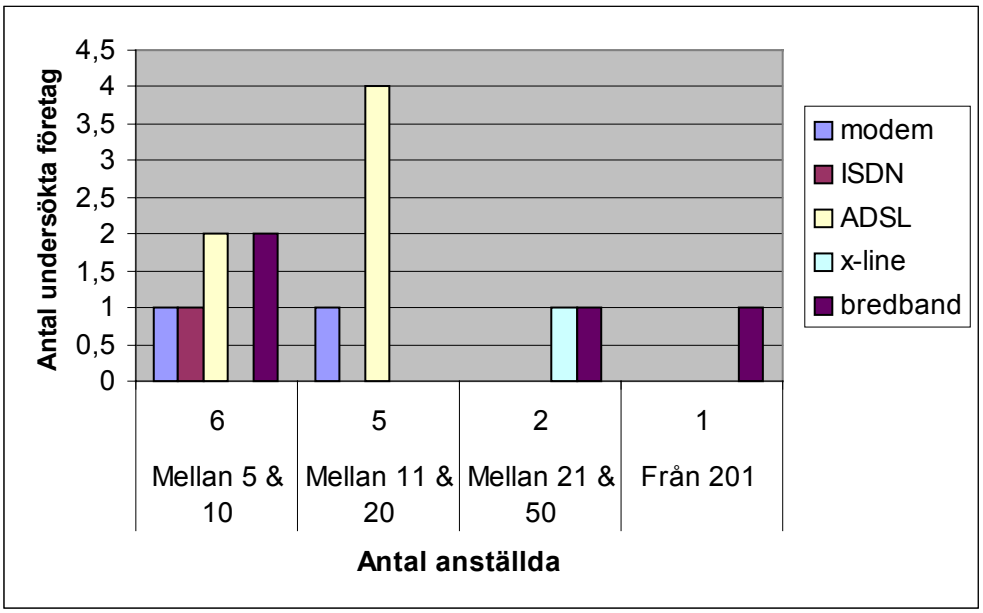
Vi har för att tydliggöra fördelningen över företagen gjort ett stapeldiagram. I figur fem visas hur många företag av varje typ som har medverkat i vår kvantitativa undersökning.



Figur 5 Stapeldiagram på fördelningen av företagen.

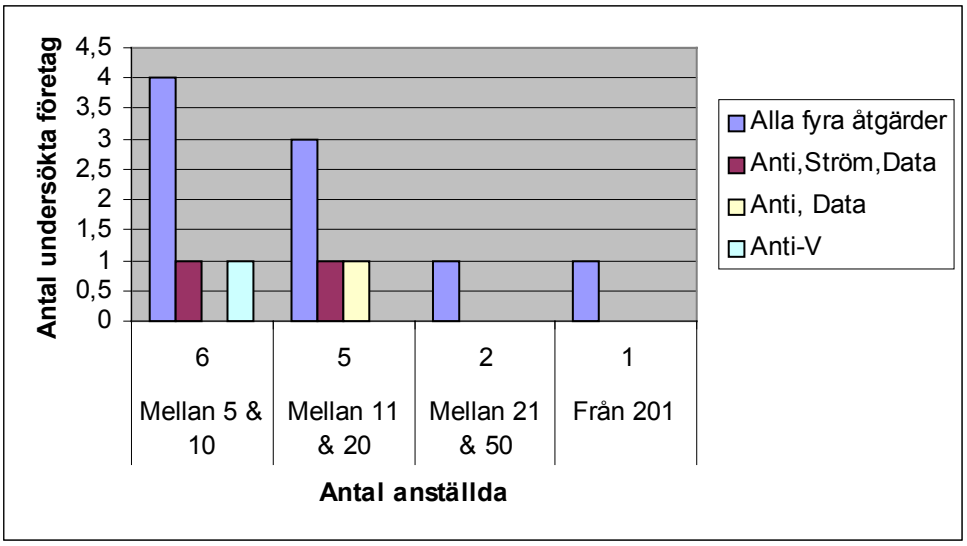
I början av enkäten, nämligen fråga 3, frågar vi om det finns någon IT-ansvarig på företaget och i sådana fall vem detta är. Anledningen till att vi ville veta namnet var för att om företaget skulle bli utvalt till att intervjuas skulle vi veta vem vi skulle prata med. Där har 93 % svarat att de har en utvald person som är IT-ansvarig medan 7 % inte har någon utnämnd. Därefter följer frågan om företaget har egen IT-drift. Med IT-drift menar vi allt från egen server till all skötsel av säkerhetsanordningar för Internet. Ett företag som inte har egen IT-drift kan tänkas antingen ingå i en koncern där driften ligger på en central plats på eventuellt huvudkontoret eller att den rentutav är outsourcad på ett externt företag. 43 % av företagen svarar att de har egen IT-drift och 57 % svarar att de inte har det.

Alla företag har tillgång till Internet och därav kommer följdfrågorna om typ av uppkoppling, vidtagna säkerhetsåtgärder etc. I figur 6 visar vi på vilken typ av uppkoppling företagen har.



Figur 6 Stapeldiagram över vilken uppkoppling de olika företagen har i förhållande till antalet anställda.

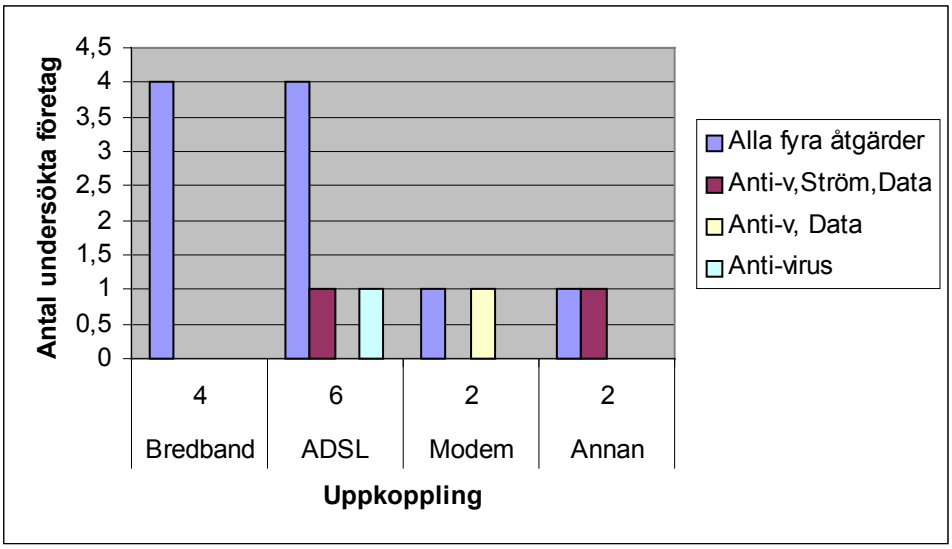
Vilka åtgärder företagen vidtagit var en av de viktigaste frågorna i enkäten. Vi åskådliggör i figur 7 hur företagen har skyddat sig och hur många anställda de har. Detta för att se hur säkerheten påverkas av företagets storlek. De åtgärder vi syftar på är Brandvägg, Antivirusprogram, ström- och databackuper.



Figur 7 Stapeldiagram över vilka åtgärder företagen har vidtagit i förhållande till antalet anställda.

Vi frågade även om alla anställda har tillgång till Internet och på 71 % av företagen har de det medan vid 29 % av företagen har de inte det. I de fakta vi har tagit del av är det många som yttrat att ju färre som använder sig av Internet desto mindre är risken att drabbas. Även på någon av intervjuerna har detta påpekats att det är en onödig säkerhetsrisk att låta fler användare än nödvändigt använda sig utav Internet.

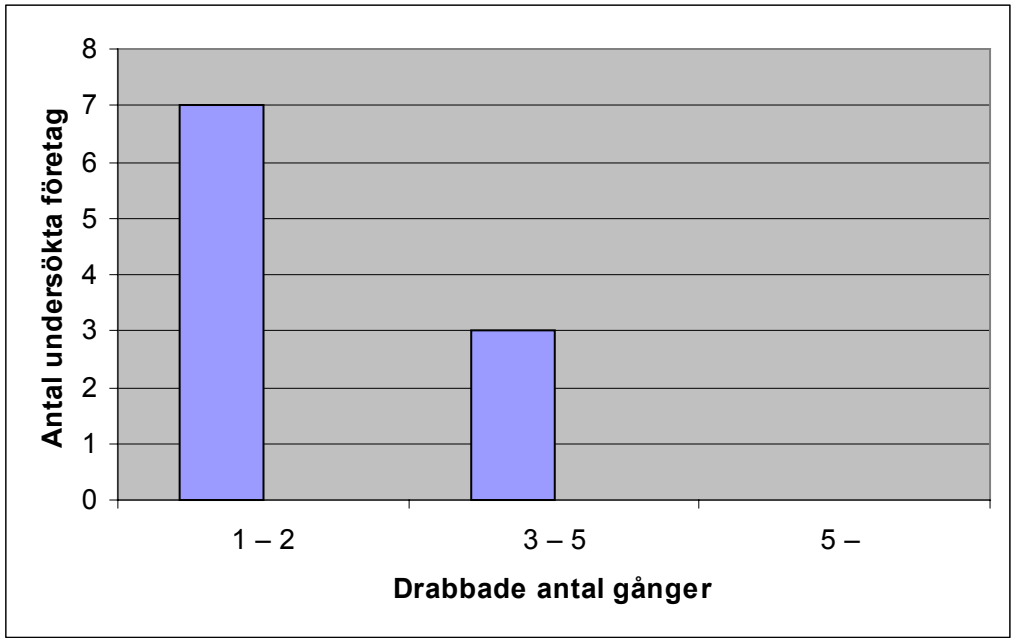
I figur 8 återger vi vilka säkerhetsåtgärder företagen vidtagit beroende på vilken uppkoppling de har. De åtgärder vi syftar på är även här Brandvägg, Antivirusprogram, ström- och databackuper.



Figur 8 Stapeldiagram över vilka åtgärder företagen vidtagit i förhållande till vilken uppkoppling de har.

Vi har även frågat om företaget har någon säkerhetspolicy för att skydda sin information. 57 % svarar att de har det och 43 % svarar att de inte har det. Nu i efterhand när vi jämför de båda undersökningarna kan denna siffra kännas något missvisande. Endast ett fåtal av företagen vi intervjuat har en säkerhetspolicy och i de flesta fall där säkerhetspolicy fanns var det frågan om ett dokument som huvudkontoret hade publicerat.

En av våra grundläggande problemställningar var just gällande virus och intrång och vi har därför frågat om de någon gång drabbats av dessa hot. För att få en bild av hur allvarligt läget är frågade vi även hur ofta de drabbats. 29 % av företagen har aldrig drabbats medan 71 % har drabbats. För att åskådliggöra fördelningen över hur många gånger företagen drabbats av virus eller intrång har vi gjort en tabell. Se figur 9.



Figur 9 Stapeldiagram över antal gånger företagen har drabbats av virus eller intrång.

Följdfrågan blir då om de gjort några ändringar ur säkerhetsperspektiv inom IT-området. Detta var inte alla lika förtjusta över att svara på eftersom det ibland klassificeras som sekretessbelagd information. Men 50 % har gjort ändringar de senaste tre åren.

För att komplettera frågan om IT-drift som vi nämnt tidigare frågade vi även mer specifikt om de hade en egen server på företaget. 64 % har egen server och 36 % har det inte. Vi frågade även om företaget tar hjälp i från någon extern organisation angående IT-frågor. Detta gjorde vi för att se hur många av företagen som var självgående i frågan om IT-kunskaper. Här får vi resultatet att 64 % gör det medan 36 % inte tar hjälp utifrån.

Till sist ville vi veta hur vanligt det var med interna utbildningar på företaget inom säkerhet. 79 % svarar att företaget inte har det och 21 % svarar att det har det. Detta kan vara en något diffus fråga eftersom vi inte ifrågasätter hur ofta eller hur omfattande utbildningen är. Om vi kontrar mot resultatet i den kvalitativa undersökningen så har det visat sig där att internutbildningar är mycket sällsynt förekommande. Om de förekommer är det oftast i anslutning till någon annan utbildning.

5.2 Intervjuundersökning

Då undersökningen är avgränsad till Dals-Ed blev antalet företag begränsat och intervjuerna omfattar därför både försäljnings-, tjänste- och producerande företag. Uppdelningen dem emellan är att hälften av företagen är producerande företag varav ett flertal av dessa även säljer sina produkter. Dvs. de är en kombination mellan försäljnings- och producerande företag. 3 företag erbjuder sina kunder olika tjänster, de är alltså tjänsteföretag. Även storleken på företagen varierar, trots vårt urval av de största företagen. Det handlar om företag där antalet anställda varierar ifrån 15 till flera hundra. Även nätverksstruktur skiljer sig mellan de olika företagen beroende på behov i företaget. Alla företag har sina kundkretsar, oberoende på företagets karaktär, som är alltifrån att vara koncentrerade till Sverige och Norden till att omfatta hela världen. Detta styrs av om företaget är en del i en koncern eller helt fristående. Fördelningen är att 3 företag är helt fristående, 3 tillhör minikoncerner medan resterande 4 tillhör storkoncerner.

IT-hantering

IT-hanteringen varierar mellan företagen. En del företag har inte en anställd som är enbart IT-ansvarig utan på några företag har en person som ursprungligen är ekonomiansvarig tilldelats uppgiften som IT-ansvarig. Respondent 2 säger: ”Det går inte att sitta här som ekonomigubbe och sen tro att du ska klara av det här med datorer.” (Anonym, 2003-09-15) Företag 2 ingår i en koncern och har en IT-ansvarig utomlands som sköter det mesta. Där lagras även all information centralt på servrar. På företag 3 har de två IT-ansvariga som sköter allt som rör IT. De är dessutom jourhavande vilket innebär att någon av dem ska kunna vara på plats inom en timme då problem uppstår. Bland företagen finns också varianten att VD: n eller delägaren/ägarna sköter IT-driften. Denna sort tillämpas på företag 10 och företag 1. Besluten om IT-hanteringen och säkerheten tas oftast av ledningen medan den IT-ansvarige rekommenderar förslag på vad som borde genomföras. Anledningen till att det inte är den IT-ansvarige som även tar besluten är att det ofta innebär mer eller mindre investeringar.

De intervjuade företagens nätverk varierar efter förutsättningar och behov. Generellt sett har de flesta företag stjärnnät, för att hanteringen av informationen ska fungera på ett så effektivt sätt som möjligt utan köbildning. Storleken på nätverken däremot varierar från att omfatta 3 datorer till flera hundra. Företag 5 har varianten att ha ett nätverk för butiksdata och ett nätverk för övrig administration och mellan dessa nätverk sker ingen kommunikation. Anledningen är att butiksdatan är baserat på dos och nätverket inte kan använda sig av fler datorer utan att omkonfigureras. Därför utvecklades ett helt nytt nätverk. Ett program som de flesta företagen använder sig av vid e-postkommunikation är Lotus Notes som är en IBM-produkt. Lotus Notes är en typ av programvara som hjälper till då kollegorna befinner sig på olika platser. Med hjälp av Notes kan de samarbeta på ett enkelt och okomplicerat sätt. Det är möjligt att skicka e-post, lagra gemensam artikelinformation och även annan information. De anställda kan se då andra användare är uppkopplade och om så önskas chatta med dem (IBM, 2003). Övriga program är olika beroende på vad företagen använder dem till. Ett som återkommer hos flera företag är dock Pyramid. Det är ett affärssystem som hanterar områdena ekonomi, administration och information. Grundmoduler i Pyramid är projekthantering, fakturering/leverantörsreskontra, order, lager, inköp, säljstöd och redovisning (Devisum, 2003). Det är vanligt att företag då även har ett annat program för de uppgifter som inte hanteras av Pyramid.

Företag 1 är en arbetsplats som i stort sett är papperslös där allt sker via datorerna så som beställningar, faktureringar, orders etc. Respondent 1 säger: ”All information lagras på en gemensam server *någonstans*.” (Anonym, 2003-09-15) Programmet Pagero används av

företag 8 för att göra löne- och leverantörsuppgifter då det krävs att de med hjälp av ett modem ringer upp respektive mottagare för att få skicka informationen. Respondenten på det medelstora företaget 10 förklarar att servern som de använder är fyra år gammal och har vållat en del problem. Den kommer därför att bytas ut inom en snar framtid. Även nätverkskablarna har börjat bli gamla och ska bytas.

Alla intervjuade företag har på ett eller annat sätt Internetuppkoppling. Det varierar från modemuppkoppling till bredbandsuppkoppling. Det medelstora företaget 1 har gått från ett analogt telefonnät till en helt digital uppkoppling där XDSL används ut mot Internet. Programmet de använder är Lotus Notes som omprogrammerats av en inhyrd programmerare för att anpassas till deras behov. Det körs på ett internt nätverk mellan de platser företaget är beläget på.

Det mer vanliga protokollet som används är TCP/IP som oftast används för trafik både ut och in till det lokala nätverket. På de flesta företag har alla anställda tillgång till Internet men respondent 2 säger: ”De anställda i produktionen har inte tillgång till Internet. Ju färre det är som har tillgång till Internet desto mindre är risken att någon gör ett misstag och visar vägen in till informationen för maskar och annan skadlig kod.” (Anonym, 2003-09-15) Företag 7 är ett stort företag och har Odette-koppling genom en egen lina som hyrs av Telia. Där används protokoll X30 och linan är en så kallad säker lina där det bara utbyts Odette-information. Det är alltså en lina vid sidan av Internet. Där görs leveransplaner och när företaget är klart med produktionen av det kunden vill ha görs en elektronisk avisering som skickas till kunden. Även fakturor kan skickas via Odette-kopplingen. På samma företag har de en så kallad RAS-uppkoppling (Remote Access) vilket innebär att någon som arbetar hemifrån kan ringa upp servern och på så sätt hämta data till den bärbara datorn. Företag 9 hade bara ett singelmodem innan de fick uppkoppling mot Internet. När detta skedde runt 96/97 behövde de tänka om helt gällande brandväggar osv.

Det vanligaste är att alla anställda har en egen inloggning och en egen identitet. Företag 1 har även på vissa datorer fingeravtrycksinloggning. Där har användarna också olika behörighet och endast några få kan lägga till och ändra i programinställningarna. På företag 6 hade de inte egna login utan istället har de 3 olika nivåer av behörighet bland användarna. Här var det endast de anställda inom butiks- och kontorsavdelningen som hade tillgång till datorerna. Hos företag 8 loggar de anställda in sig i Pyramid på morgonen och låter det stå öppet hela dagen eftersom de inte gör skillnader på behörigheter. Företag 10 kräver användarnamn och lösenord som varje användare har för att de ska komma in i systemet men det är inte så viktigt att logga ut vid lunch utan om inloggning skett förblir det så hela dagen. Medan det hos andra är som regel att de anställda ska ha loginskärmsläckare och alltid logga ut när de lämnar datorn eller rummet, som exempelvis på företag 7.

Säkerhetspolicy

Synen på säkerhetspolicy är delad bland företagen, det är dock ingen som har en policy som är väl dokumenterad eller förankrad i företaget. På fem av tio företag saknar de helt säkerhetspolicy. I företag 7 har de en så kallad Internet- och E-postpolicy, vilket innebär att allt som sker på Internet och all e-post som skickas är företagets officiella information. De har ingen direkt säkerhetspolicy och den de har rör i så fall de anställda som har bärbar dator. Men detta innebär inga begränsningar på så sätt att de inte får ta med sig datorn överallt eller ta med sig data någonstans. De kommer dock troligen att få en säkerhetspolicy vid införandet av fast lina. De får inte heller diskutera datorsystem via telefon med någon som ringt upp, utan enbart om de själva tagit kontakten eller bjudit in någon till företaget. Företag 2 som är

en del av en koncern har ingen egen säkerhetspolicy skriven utan den finns centralt på huvudkontoret. Systemet är även av säkerhetsskäl byggt så att de i Sverige inte kan lägga in några program eller liknande utan huvudkontorets godkännande.

Företag 1 anser att de anställda är mycket väl medvetna om den säkerhetsrisk som innebär att vara ute på Internet. De får information via e-post och de vet även om att de blir loggade. Företaget loggar all information som sker ut från företaget men inte den ingående trafiken eftersom det hade blivit för mycket. En tidigare anställd försökte skicka in virus men istället blev han loggad och de kunde snabbt oskadliggöra honom. På företag 10 loggas användarna av Internet automatiskt men det kollas aldrig. Respondenten på företag 3 berättar att de anställda får vissa restriktioner om vilka program som får och vilka som inte får installeras, detta pga. att det inte ska bli kompatibilitetsproblem med något av systemprogrammen. Samma person säger också när vi frågar om säkerhetspolicyn: ”En sak är att de måste byta lösenord med jämna mellanrum och det måste innehålla ett visst antal tecken.” (Anonym, 2003-09-15) Företaget loggar inte sina anställda på något sätt, det enda som görs är att effektiviteten kontrolleras på de anställda med hjälp av olika metoder baserat på deras verksamhet. Alla anställda får information om vad de får göra och inte göra genom en introduktionskurs. De får även en handbok över vilka regler som finns. En annan säkerhetsåtgärd som införts är ett passerkortsystem, vilket gör att inga obehöriga kommer in.

Företag 9 säger att de inte har någon dokumenterad säkerhetspolicy men funktionen finns. Anledningen till bristfällig dokumentation är brist på tid.

Bandbackuper
När information lagras är det inte en fråga om någonting kommer att hända utan NÄR. Detta innebär först och främst att en backup på informationen bör göras. Företagen vi har intervjuat har alla varit medvetna om detta och använder sig av så kallade bandbackuper som kan lagra stora mängder information beroende på vilken typ av band som används. Hur noga det sköts och vilka rutiner för vart banden lagras etc. är däremot olika från företag till företag. Företag 1 som vi intervjuade var mycket noga inom detta område. De angav inte vart servern som de använde sig av fanns eller vart banden förvarades bara att det fanns på olika adresser. De hade även en diskspegling vilket gjorde att arbetet i princip aldrig skulle behöva avbrytas och att om något skulle hända skulle i bästa fall endast de senaste minuternas arbete gå förlorat och i värsta fall de senaste timmarna. Några andra företag var inte lika noga med backuperna. Respondent 8 svarade: ”Här…skratt…i en väska. Jag vill ha något speciellt att ha bandbackuperna i, annars glömmer jag dem på hyllan hemma när jag åker till jobbet.” (Anonym, 2003-09-17) Övervägande företag förvarade banden i ett brandsäkert skåp under natten. Generellt sett valde nästan alla företag utom två att göra backup på informationen som fanns lagrad varje natt. Ett av dessa företag som inte gjorde backup varje natt var företag 2 som gjorde det en gång varje vecka och det andra var företag 6 som bandade informationen varje tisdag, onsdag och torsdag.

Strömbackup
Alla responderande företag har en strömförsörjande backup ifall det blir strömavbrott. Storleken på dessa varierade något från att hålla igång hela nätverket till att endast hålla igång servern. Kvaliteten varierade också. En del företag hade strömbackup i fem minuter och en del upp till en timme. Företag 3 hade även ett dieselaggregat som kunde hålla verksamheten igång under en längre period.

Brandvägg
Att använda sig utav en brandvägg för att säkra sin information och skydda sig var inte riktigt lika självklart. Åtta av tio företag använde sig av brandvägg. Företag 1 hade en mycket intelligent säkerhetslösning med två brandväggar mellan Internet och det interna nätverket som kommunicerar med varandra i ett annat tjänsteprotokoll än TCP/IP. Detta för att öka säkerheten mot intrång. Respondent 10 visste med sig att brandväggen borde ha omkonfigurerats för länge sedan och att den mer fungerade som ”en mur” än vägg. Två företag som inte använde sig av brandvägg är företag 6 som har uppkoppling via ADSL och företag 4 som använder sig utav modem. Vi fick följande svar från respondent 8: ”Ja, vi har brandvägg. Men den vet jag ingenting om.” (Anonym, 2003-09-17) Brandväggen behöver inte bara finns där som ett skydd utåt utan även för att kontrollera trafiken från insidan. Denna funktion använde sig bl.a. företag 1 av.

Antivirusprogram
Det som det har varit mest skriverier om i nyheter och tidningar den senaste tiden vad gäller informationssäkerhet har varit alla varningar för virus, maskar och trojanska hästar. För att skydda sig mot att de tar sig in i nätverket och systemen krävs det en medveten användare men även ett bra virusskydd. Alla företag hade antivirusprogram av lite olika fabrikat och uppdaterar detta relativt ofta. För att underlätta arbetet och för att inte glömma bort att uppdatera hade de flesta företag automatisk uppdatering. Företag 3 hade ett avtal med ett antivirusföretag som gjorde att de fick uppdateringar om nya virus dygnet om. Annars var det lite olika. På frågan om hur ofta uppdateringarna görs får vi följande svar från respondent 6: ”Ja du, hur ofta har jag satt det på? Men det är rätt ofta faktiskt.” (Anonym, 2003-09-16) Medan respondent 7 säger: ”Ungefär 1 timme om dagen går åt till att se till att vi har rätt skydd.” (Anonym, 2003-09-17)

Företag 9 har ett Antivirusprogram på alla servrar och även på klienter genom e-postsystemet. Uppdateringar skickas automatiskt till användaren då de loggar in. I programmet talar de om vilka användare som ska få uppdateringar. Har användaren inte funnits med på listan tidigare skickas hela programmet och signaturfilen ut över de virus som den ska känna igen. Nästa gång de loggar in jämförs signaturfilen med det som är uppdaterat på servern, är det inte senaste uppdateringen skickas nya uppdateringar.

Extern hjälp
För att kunna upprätthålla säkerheten är det relativt vanligt att företag tar hjälp av utomstående företag för att konfigurera olika delar av nätverket. Även de företag som i vanliga fall sköter all typ av serverdrift själva har ibland tagit hjälp för att t.ex. konfigurera brandväggen vid installation. En del av företagen vi har intervjuat som idag har egen serverdrift skulle kunna tänka sig att i framtiden låta något annat företag ta hand om IT-driften eftersom det tar mycket tid att sköta det själv.

VPN/kryptering
Företag som ingår i olika koncerner eller har ett nära samarbete med andra företag skickar ofta information om uppdrag etc. mellan olika platser. Om denna information är krypterad eller inte är lite olika. Vissa företag är mycket noga med att all trafik ute på allmänna nät är krypterad medan andra företag inte reflekterar över att andra kan läsa informationen som skickas. Företag i större koncerner med kontor i andra länder, som har nätverk som kommunicerar med varandra är i regel mycket noggranna. Exempelvis företag 1 som använder sig av VPN-lösningar mellan kontoren och krypterar information som skickas via WLAN m.h.a. handdatorer. Inne i dessa nätverk kontrolleras även alla datorer med IDS som

läser av alla enheterna så att det inte finns några gömda virus, maskar eller trojanska hästar. Respondent 1 säger: ” Man kan sitta och skryta med att man är hur säker som helst. Men låt säga att man inte klarar av en trojan som någon skickar in så ligger den inne och skickar ut upplysningar hela tiden. Så att scanna efter sådana är något som går dygnet runt hos oss.” (Anonym, 2003-09-15) Respondenten pratar om ett intrångsdetekteringssystem som avläser trafiken och söker efter misstänksam aktivitet. Av de företag som vi har intervjuat finns företag som endast har viss kontakt med andra företag och ev. systerbolag m.m. krypterar inte sin information. Tre företag använder sig av VPN-lösningar, nämligen företag 1, 2 och 3.

Drabbade
Tre av företagen som vi har intervjuat har någon gång blivit drabbade av intrång eller virusattacker, en del mer frekvent än andra. Ett av dessa var företag 10 som drabbades för inte så längesedan då hela servern fylldes av temporära filer och hela nätverket kopplades ner. Det tog två dagar att få ordning på datorerna igen men det blev inga skador i form av förlorad information bara förlorad inkomst. Samma respondent sa: ”Vi är så få här så då skriker man när man fått ett virus och så kommer någon och hjälper. Det brukar fungera. En som håller på med försäljning får rätt så mycket från externa parter, varannan vecka ungefär. Så det blir lite attacker då och då.” (Anonym, 2003-09-22)

Respondent 3 kommenterade att det var betydligt lättare att skydda sig från intrång utifrån nätverket än vad det är att skydda sig mot dem som redan är inloggade i nätverket. Tyvärr finns det anställda som ibland vill utföra saker som de inte har behörighet till. En av företag 1:s samarbetspartner fick ett virus och eftersom flera av de anställda fanns med i det smittade företagets anställdas adressböcker fick de ett antal e-post innan deras server kopplade ner, men viruset kom aldrig in i deras nätverk. Respondent 1 säger: ”Det förekommer säkert 100 försök varje dag av scanners som kollar av öppna portar. De blir vi också träffade av, alla blir träffade av dem.” (Anonym, 2003-09-15).

6. Diskussion och analys

När vi började vårt arbete utgick vi från att företag i Dals-Eds kommun hade en låg medvetenhet om hoten och vikten av ett gediget säkerhetsarbete för att skydda sig och sin information. Vi har förstått att mindre företag ibland har bristande IT-kunskaper och därmed även försummat säkerhetsarbetet. Om detta beror på att de är företag i glesbygd eller om det endast beror på att de är *små* företag är svårt att utläsa då vi inte har fakta för att kunna jämföra med små företag i större kommuner. Den information vi har fått från GM:s tidigare forskning visar att säkerhetsarbetet generellt är bristfälligt i mindre företag men om dessa företag är belägna i större eller mindre kommuner får vi inga uppgifter om. Vi vill därför påstå att säkerhetsnivån ligger under medel hos mindre företag i allmänhet. Vi har ibland mött inställningen hos respondenter på mindre företag att de anser sig ha så lite information eller ointressant information för utomstående och därför tycker att mer omfattande säkerhetsarbete inte är lönsamt. Vi anser att informationen är en del av företagets resurser som förutsätter deras existens. Därför är säkerhetsarbetet viktigt i alla företag, stora som små.

I vår kvantitativa undersökning hade hälften av företagen en säkerhetspolicy. Detta resultat överensstämmer med den tidigare forskningen vi studerat. Vad som bör uppmärksammas är att vi i vår kvalitativa undersökning märkt att synen på säkerhetspolicy varierar stort. Företagens uppfattning av en policy kan sträcka sig från att tala om för användaren att lösenord ska bytas regelbundet till att beskriva hur ett mer omfattande säkerhetsarbete ska fungera med ansvarsområden etc. Dvs. att företag som säger sig ha en policy ibland inte har

den tillräckligt utvecklad för att fylla rätt funktion eller att användarna aldrig har fått ta del av den. De företag som har en mer omfattande policy är företag som är större eller som ingår i större koncerner.

Vi har en teori om att säkerhetsarbetet påverkas till stor del av delarna medvetenhet, säkerhetspolicy och handling. Om företaget har en hög medvetenhet om riskerna informationen utsätts för bidrar det till handling på så sätt att de vidtar åtgärder. För att kunna vara medveten om vilka åtgärder som är relevanta bör en säkerhetspolicy ha genomarbetats där hoten prioriterats. I vår kvalitativa undersökning framkom det att få företag har en genomarbetad säkerhetspolicy och eftersom detta är en av de viktigaste delarna i säkerhetsarbetet då det påverkar handlingarna finner vi att medvetenheten ligger under medel hos dessa företag.

En brist i många företag handlar om att de saknar en person som enbart är IT-ansvarig. I vår enkätundersökning framkom det dock att 93 % av de medverkande företagen hade en utsedd IT-ansvarig. Denna siffra kan vara något missvisande pga. att när vi pratar om vikten av att ha en IT-ansvarig syftar vi på en person med kvalificerade kunskaper om datorer och nätverk. Det visade sig i intervjuundersökningen att de flesta företagen hade en IT-ansvarig men den personen saknar ofta de egenskaper vi önskar att en den hade. Vi har då tolkat detta resultat som att de saknar en kvalificerad IT-ansvarig. Anledningen till att 93 % svarar i enkäten att de har en IT-ansvarig är troligtvis grundat i att de anser sig ha en IT-ansvarig oavsett om det är en person med IT-kunskaper eller en ekonomianställd som fått det uppdraget. Vi kan se ett samband mellan olika typer av organisatoriska hot i företagen pga. en otydlig roll- och ansvarsfördelning. Detta relaterar vi till teorin och ser att i de fall vi stött på, där företag saknar ovanstående fördelning har de också drabbats av intrång eller virus pga. användarens misstag. Ett exempel är företag 10 som inte har någon anställd som enbart är IT-ansvarig och de får in virus med jämna mellanrum, det var också hos detta företag som systemen stod stilla i två dagar pga. en virusattack. Anledningen till att användarna gör dessa misstag grundar sig troligtvis i att de inte vet vem de ska vända sig till eller hur de ska hantera systemen på ett säkert sätt. Företaget placerar vi under kategorin låg medvetenhet pga. att deras brandvägg inte har den funktionalitet som den borde ha. Detta kan vara en bidragande orsak till att de får in virus med jämna mellanrum. De saknar en väl förankrad säkerhetspolicy och deras fysiska nätverk skulle ha bytts ut sen en tid tillbaka.

Det framkommer att 70 % av företagen i enkätundersökningen respektive 30 % i intervjuundersökningen någon gång drabbats av virus eller intrång. Detta är en stor skillnad vilket vi tror kan bero delvis på vårt bortfall i enkätundersökningen. En annan orsak till dessa siffror kan vara att de företagen i enkätundersökningen uppgett att de drabbats av virus eller intrång även om de kunnat blockera viruset/intrånget innan de orsakat någon skada. Detta framkom inte av enkäten medan vi under intervjuerna tolkade ett sådant svar som att de ej drabbats av virus.

Det största hotet som föreligger för de undersökta företagen är kanske inte förlust av data då alla använder sig både av band- och strömbackuper för att säkra sin information. Utan det som är av störst vikt är att se till att produktionen eller systemen inte blir stillastående pga. att servern eller datasystemen överbelastas. Det är även viktigt att företagen inser att de faktiskt har information som de inte vill att någon obehörig ska kunna se eller stjäla så som lönehantering, fakturering, leverantörshantering etc. Detta gäller framförallt företag 4 och 6.

Vi har stött på hos företag 3 ett av de svåraste hoten att skydda sig mot, nämligen intrång inifrån. Detta är en typ av logiskt hot. Det kan tänkas att om ett företag har förankrat sitt säkerhetsarbete hos alla de anställda så borde dessa risker vara minimala då det oftast är den mänskliga faktorn som är orsaken. Trots att detta var ett av de företagen med ett omfattande säkerhetsarbete och hög medvetenhet om vikten att skydda sig blev de drabbade. Detta visar hur svårt det är att skapa ett hundraprocentigt skydd, än så länge är ju detta omöjligt. En anledning till att de drabbades kan ha varit en liten brist i förmedlingen av företagets säkerhetskultur. Det kanske inte räcker med att skicka information per e-post utan att det behövs internutbildningar i informationssäkerhet. Ytterligare ett exempel är återigen företag 10 som utsatt sig för en annan typ av hot. Närmare bestämt ett fysiskt hot, där servrarna och kablarna var gamla och hade orsakat problem. Nu skulle både servern och kablarna bytas ut men att låta det gå så långt att problem uppstår är en stor miss i säkerhetstänkandet. Detta visar på att insikten om att en åtgärd krävs kommer för sent. Istället för att förekomma ett sådant här hot, vilket inte är särskilt svårt att göra tillåts problemen uppstå innan åtgärder tas.

De punkter som vi tagit upp i teoriavsnittet ADB-säkerhet och kommunikationssäkerhet är bra att fundera över då nya program ska utvecklas eller inköpas. Fyller programmet dessa säkerhetskriterier eller måste vissa prioriteras bort beroende på kostnad? Hos de företag vi har intervjuat kommer ADB-säkerheten in på ett eller annat sätt eftersom alla företag är angelägna om att skydda informationen från obehöriga osv. Kommunikationssäkerheten är det endast några företag som har tagit hänsyn till. Bl.a. företag 7 med Odette-koppling och företag 1,2 och 3 som använder sig utav VPN. Dessa fyra företag är de vi skulle ha placerat under kategorin hög medvetenhet om de hade haft en säkerhetspolicy utformad efter Mitrovic´ (2001) rekommendationer. Företagen har möjligtvis en hög medvetenhet om hoten och har handlat därefter, men vi menar att en säkerhetspolicy hade bidragit till större förståelse och medvetenhet bland övriga anställda. De anställdas handlingar kan inte styras utan enda sättet att skydda sig mot deras möjliga felsteg är att göra dem medvetna om konsekvenserna. På grund av detta kan vi inte placera dessa företag under en högre kategorinivå än medel.

Alla företag omfattade av våra intervjuer och enkäter har ett antivirusprogram installerat. Detta är mycket positivt då det är ett av de grundläggande skydden. Utan ett antivirusprogram skulle det vara oerhört svårt att klara sig med ett nätverk som är uppkopplat mot Internet idag. Det är även lugnande att se att alla uppdaterar det trots att intervallerna varierar. Det som inte verkar ha nått fram hos alla företag är vikten av att installera en brandvägg. Det är möjligt att ett företag med modemuppkoppling inte är lika utsatt och därmed inte heller är av så stort behov av en brandvägg. Dock saknar även företag 6 som har ADSL brandvägg, vilket vi tycker är en stor brist i säkerhetsarbetet då detta kan bidra till att andra obehöriga på Internet använder sig utav datorns resurser genom att lagra olagligt material t.ex. barnpornografiska bilder eller använda datorn till att utföra olagliga handlingar. Vi har fått uppfattningen om att det beror på att de helt enkelt inte anser sig behöva någon brandvägg. I sin tur vill vi påstå att det grundar sig i bristfälliga IT-kunskaper och omedvetenhet om vilka hot de är utsatta för. Återigen trycker vi därför på betydelsen av en utsedd IT-ansvarig med kunskaper inom detta område med stöd av Mitrovic´ s (2001) roll- och ansvarsfördelning. Grundat på detta placerar vi företag 6 under kategorinivån låg medvetenhet. Där hamnar även företag 4 som också saknar brandvägg och säkerhetspolicy.

Företag 5, 8 och 9 har vidtagit de åtgärder som uppfyller kraven för kategorinivån medel medvetenhet. Då de saknar säkerhetspolicy menar vi att de ligger på gränsen till låg medvetenhet även om respondenterna hade grundläggande IT-kunskaper. En anledning till att

företag 8 inte är så noga med inloggning och utloggning kan vara att de saknar säkerhetspolicy vilket speglar deras handlingar.

Vi kan se tendenser av att de företag som har vidtagit mer avancerade säkerhetslösningar är större företag som ofta ingår i större koncerner med kompetenta personer som ansvarar för IT-hanteringen. Det beror troligen på att de har mer resurser att utnyttja än vad mindre företag har. De har ofta även mer komplexa system som kräver mer underhåll. Vi har stött på funktionen med IDS hos företag 1. Detta företag samt ytterligare några företag anser vi ha ett gediget säkerhetsarbete. Det är dessa som har kunskapen om vad som vilka hot som föreligger och vad som kan göras mot dessa. Även de företag där vi får uppgifter om att kryptering och VPN-lösningar används, är dessa företag. Trots att många mindre företag kommunicerar och skickar information över Internet mellan kunder, leverantörer och samarbetspartners använder de sig inte av kryptering. Detta visar också på att säkerhetstänkandet i dessa företag är bristfälligt.

7. Slutsats

Utefter våra resultat kan vi dra slutsatsen att vi inte har funnit tillräckligt med stöd för vår hypotes för att kunna påstå att den är sann. Vi anser inte att säkerhetsmedvetenheten är låg eftersom endast tre av tio företag hamnat under den kategorin. Däremot skulle vi vilja att medvetenheten generellt sett låg på en högre nivå än den gör idag. Detta innebär att vi falsifierar vår hypotes. Vi har hittat mönster bland de undersökta företagen som visar att medvetenheten om säkerhetsarbetet är lägre hos små företag och drar därmed syntesen att säkerhetsarbetet påverkas av företagens storlek och nätverkens storlek. Pga. detta varierar naturligtvis även nivån på medvetenheten. De företag som har större nätverk och fler anställda är oftast de mest utsatta då riskerna ökar ju fler användarna är. Men vi vill dock inte förringa vikten av att även mindre företag blir underförstådda med riskerna och därmed ökar sitt säkerhetsarbete. Det skrämmande i vår undersökning är att det faktiskt finns företag som har uppkoppling mot Internet men som saknar grundläggande säkerhetsåtgärder. Även att företagen tar så lätt på attacker av virus är obehagligt eftersom virusen idag är så oerhört många och i princip alla som har uppkoppling mot Internet någon gång träffas av dessa. I vårt resultat kan vi se att många företag brister i att informera sina anställda och vi drar därför slutsatsen att internutbildningar är något som måste förbättras på företagen för att säkerhetsarbetet överhuvudtaget ska fungera. Annars blir det en motverkande effekt som beror på att företaget inte gett de anställda tillräckligt med instruktioner om säkerheten.

Sammanfattningsvis anser vi att trots saknaden av stöd för vår hypotes kan slutsatsen dras att säkerhetstänkandet hos företag i Dals-Ed idag inte ligger på den nivå det borde göra. Det vi har sett är att de stora företagen har insett vikten av ett gediget säkerhetsarbete medan de mindre företagen har en bristande förståelse för de hot som föreligger och därmed även har ett bristfälligt säkerhetsarbete.

8. Förslag till vidare forskning

Som vi tidigare sagt har vi sett att mindre företag är de som inte har det säkerhetsarbetet de borde. Nu är vår undersökning avgränsad till Dals-Ed och vi kan därför inte svara för hur det ser ut i övriga landet. Det skulle därför vara av intresse att försöka utreda huruvida våra resultat överensstämmer med säkerhetstänkandet även i andra delar av landet. Våra studier i tidigare forskning visar att det gör det men eftersom dessa studier inte talar om var de undersökta företagen är belägna mer än att det är i Norden vet vi inte hur relationen är mellan

säkerhetstänkandet och glesbebyggelse eller tätbebyggelse. En intressant studie att göra är därför en jämförande undersökning där tätort kontrar glesbygd.

9. Referenser

Ahlberg, J. (2003). *Virus och datorsäkerhet* [www dokument]. URL http://www.jonasweb.nu/datorn/virus.html

Andersson, H. (1999). *IT-säkerhet – En kort PM om de teoretiska och tekniska grunderna* [online]. Tillgänglig: Juridicum [6 oktober 2003]

Almgren, Å. & Johansson, T. (2003). *Brandväggar1* [www dokument]. URL http://www.hh.se/staff/jovall/secure/bidrag_2/wall1/firewall_1.html

Arnesjö, P. (2000). *Begrepp om ADB-säkerhet* [www dokument]. URL http://194.165.231.32/hemma/parnesjo/adb-sak/begrepp/begrepp.htm

Atremo (2003). *Vad är en brandvägg?* [www dokument]. URL http://www.atremo.se/isite-cache/filer/130/Introduktion_Brandv%E4ggar.pdf

Backman, J. (1998). *Rapporter och uppsatser.* Lund: Studentlitteratur.

Befring, E. (1994). *Forskningsmetodik och statistik.* Lund: Studentlitteratur.

Carling, M. (2003). Antivirus på nytt vis – så skyddar du dig smartast. *Nätverk & Kommunikation,* nr 11?, 38-39.

Danielsson, L. (2003). Alla måste veta vem de ska prata med. *Computer Sweden,* TEMA Säkerhet, 3.

Devisum (2003). *Pyramid.* [www dokument]. URL http://www.devisum.se/sida3b.asp?val=68&sida=255

Dimension (2003). *Saknar din affärsverksamhet en Informationssäkerhetspolicy?* [www dokument]. URL http://www.dimension.se/sakerhetspolicy.html

Eneroth, B. (1984). *Hur mäter man ”vackert”? Grundbok i kvalitativ metod.* Stockholm: Akademilitteratur.

Eriksson, L.-T., & Wiedersheim-Paul, F. (2001). *Att utreda forska och rapportera* (7: e uppl.). Malmö: Liber Ekonomi.

Esser, L., & Svenjeby, R. (2003). *Säkerhetsarkitektur för ökat säkerhetsmedvetande.* (Examensarbete i datavetenskap). Högskolan Trollhättan/Uddevalla, Institutionen för informatik och matematik, 461 29 Trollhättan.

Ficora (2003). *Kommunikationssäkerhet* [www dokument]. URL http://www.ficora.fi/ruotsi/tietoturva/symmetrinen.htm

Fjordvang, P. (2002). *Säkerhet på pc och Internet.* Sundbyberg: Pagina Förlags AB.

Gääw, C. & Lindström, M. *Brandväggar* [online]. Tillgänglig: http://medieteknik.bth.se/mt00mli/firewall/Firewall.pdf [6 oktober, 2003]

IBM (2003). *IBM Lotus Notes* [www dokument]. URL http://www.lotus.com/products/product4.nsf/wdocs/noteshomepage?OpenDocument&cwesite=notes

IT-säkerhet glödhett efter 11 september. (2002, 12 september). *Nerikes Allehanda*, s. 6.
Lantz, A. (1993). *Intervjumetodik – Den professionellt genomförda intervjun.* Lund: Studentlitteratur.

Mitrovic´, P. (2001). *Handbok i IT-säkerhet.* Sundbyberg: Pagina Förlags AB.

Oppliger, R. (1999). *Security technologies for the World Wide Web.* London: Artech House.

Pagina (2003). *Proxy* [www dokument]. URL http://www.pagina.se/itord/default.asp?SokOrd=proxy

PKI-Forum (EdvinaAB) (2003). *Kryptering är matematik och politik i kombination* [www dokument]. URL http://www.pki-forum.com/intro/krypto.shtml

Safeit (2003). *Brandvägg* [www dokument]. URL http://www.safeit.com/se/skola/lektion4.html

Strebe, M., & Perkins, C. (2002). *Brandväggar 24sju* (2:a uppl.). Sundbyberg: Pagina Förlags AB.

Strömquist, S. (1999). *Uppsatshandboken* (2:a uppl.). Göteborg: Hallgren & Fallgren Studieförlag AB.

Svidén, H. (2003). Härifrån styrs virusjakten. *Computer Sweden,* TEMA Säkerhet, 14-15.

Symantec (2003). *Intrångsdetektering - vad är det?* [www dokument]. URL http://www.symantec.com/region/se/corporate/ids1.html

Symantec (2003*). Integrerad säkerhet: Ett nytt synsätt för en ny tid*. [www dokument]. URL http://www.symantec.com/region/se/corporate/integrated_approach.html

Symantec (2003). *Nordiska småföretagare okunniga om it-säkerhet.* [www dokument]. URL http://www.symantec.com/region/se/press/n030520_se.html

Trost, J. (1997). *Kvalitativa intervjuer* (2:a uppl.). Lund: Studentlitteratur.

Wallhoff, J. (2002). *Focus on informationsecurity and IT-management – trust your information* [online]. Tillgänglig: Scillani information [1 oktober 2003]

Westerlund, L. & Åström, Å. (2001). *Public Key Infrastructure – kan ett systeminförande med PKI förbättra rutiner avseende IT-säkerhet?* [online]. Tillgänglig: http://epubl.luth.se/1404-5508/2001/141/LTU-SHU-EX-01141-SE.pdf [5 oktober 2003]

Bilaga 1 - Enkätundersökning

Enkätundersökning – Datasäkerhet

(För att markera kryssrutorna högerklicka på vald ruta, välj Egenskaper och välj Markera.)

1. Vilken bransch verkar företaget inom?

Tjänsteföretag ☐

Varuproducerande företag ☐

Säljande företag ☐

Annat……...

2. Hur många anställda är det på ert företag?

1 – 5	☐	51 – 100	☐
6 – 10	☐	101 – 200	☐
11 – 20	☐	200 –	☐
21 – 50	☐		

3. Finns det någon IT-ansvarig på företaget?

Ja ☐
Nej ☐

4. Har företaget egen IT-drift eller är det utlagt på entreprenad?

Ja ☐ Om Ja, vem:…….
Nej ☐

5. Har företaget tillgång till Internet? (om inte gå vidare till fråga 10)

Ja ☐
Nej ☐

6. Har alla anställda tillgång till Internet?

Ja ☐
Nej ☐

7. Vilken form av uppkoppling har företaget?

Fast uppkoppling ☐

ADSL ☐

Modem ☐

Annan:…….

8. Har företaget egen server?

Ja ☐
Nej ☐ Om inte vilken operatör:……..

9. Har företaget någon säkerhetspolicy för att skydda sin information?

Ja ☐
Nej ☐

10. Gjordes några ändringar i säkerhetshanteringen i samband med att ni installerade Internet? I så fall vad?

Svar:……

11. Har ni hjälp från någon extern organisation angående IT-frågor?

Ja ☐
Nej ☐

12. Har företaget någon gång drabbats av någon typ av intrång eller virus?
(Om nej gå vidare till fråga 13)

Ja ☐ Om ja, vad:……..
Nej ☐

13. Hur många gånger har företaget drabbats de 3 senaste åren?

1 – 2 ☐
3 – 5 ☐
5 – ☐

14. Har det gjorts några ändringar ur säkerhetsperspektiv de senaste 3 åren inom IT-området? I så fall vad?

Svar:……

15. Kryssa i de säkerhetsåtgärder som företaget vidtagit:

Brandvägg ☐

Antivirusprogram ☐

Strömbackup ☐

Databackup ☐

Annat:……..

16. Har ni någon internutbildning för personalen i datasäkerhet?

Ja ☐
Nej ☐

Tack för er medverkan!

Jenny Olsson
Jenny Bengtsson

Bilaga 2 - Intervjumall

Intervju– Datasäkerhet

Företagets karaktär

- Berätta om företaget.
  - Typ av företag
  - Antal anställda
  - Företagets struktur
  - Koncern

IT

- Egen IT-drift eller outsourcat?
  - Vart?
- Struktur:
  - Antal datorer/enheter
  - Topologi
  - Protokoll
  - Operativsystem
  - Samarbete med annat företag → gemensam programvara
    → kryptering
- Vem är IT-ansvarig?
  - Arbetsuppgifter
  - Beslut angående IT-enheten
- Har anställda tillgång till Internet?
  - Vem/vilka arbetsgrupper
- Genomfördes ändringar i samband med att Internet installerades ?
  - Vilka ändringar?

Säkerhet

- Har företaget någon säkerhetspolicy?
  - Känner alla anställda till den?
  - Uppföljning av säkerhetspolicy?
  - Internutbildning i säkerhet?
  - Användarkonto?
    - Är datorn alltid under uppsikt då du är inloggad?
  - Loggas användarna?
    - Vet de om det?
- Vilka säkerhetsåtgärder har vidtagits?
  - Brandväggar
  - Antivirusprogram - uppdatering
  - Bandbackuper
    - Uppdatering
    - Adress

    - Strömbackuper - uppdatering
- Har det gjorts några ändringar i säkerheten de senaste åren?
- Hjälp från något externt företag?
- Har de drabbats av något säkerhetshot?
    - Typ?
    - Omfattning?
    - Förluster?
    - Förändring i säkerhetsarbetet efteråt?

Bilaga 3 - Enkätresultat

Resultat från enkätundersökningen

1. Vilken bransch verkar företaget inom?	Tjänsteföretag	5
	Varuproducerande företag	5
	Säljande företag	4
	Annat	
2. Hur många anställda är det på ert företag?	5 – 10	6
	11 – 20	5
	21 – 50	2
	51 – 100	
	101 – 200	
	201 –	1
3. Finns det någon IT-ansvarig på företaget?	Ja	13
	Nej	1
4. Har företaget egen IT-drift?	Ja	6
	Nej	8
5. Har företaget tillgång till Internet?	Ja	14
	Nej	
6. Har alla anställda tillgång till Internet?	Ja	10
	Nej	4
7. Vilken form av uppkoppling har företaget?	Fast uppkoppling	4
	ADSL	6
	Modem	2
	Annan	2
8. Har företaget egen server?	Ja	9
	Nej	5
9. Gjordes några ändringar i säkerhetshanteringen i samband med att ni installerade Internet? I så fall vad?		
10. Har företaget någon säkerhetspolicy för att skydda sin information?	Ja	8
	Nej	6
11. Har ni hjälp från någon extern organisation angående IT-frågor?	Ja	9
	Nej	5
12. Har företaget någon gång drabbats av någon typ av intrång eller virus?	Ja	10
	Nej	4

13. Hur många gånger har företaget drabbats de tre senaste åren?	1 – 2	7
	3 – 5	3
	5 –	
14. Har ni gjort några ändringar i säkerhetsarbetet de tre senaste åren?	Ja	7
	Nej	7
15. Kryssa i de säkerhetsåtgärder som företaget vidtagit:	Brandvägg, Anti, Ström, Data	9
	Anti,Ström,Data	2
	Anti, Data	1
	Anti-V	1
	Annat	
	Ej svar	1
16. Har ni någon internutbildning för personalen i datasäkerhet?	Ja	3
	Nej	11