Datasäkerhetsmedvetenhet

- en komparativ studie mellan två svenska företag

Lunds universitet
Informatik

Kandidatuppsats, 10 poäng, inom det systemvetenskapliga programmet

Framlagd: Juni-2007

Författare: Daniel Berntsson
Oskar Grunning

Handledare: Anders Svensson

Examinatorer: Mia Sassén
Erik Wallin

LUNDS UNIVERSITET
Institutionen för Informatik

Datasäkerhetsmedvetenhet

- en komparativ studie mellan två svenska företag

Daniel Berntsson
Oskar Grunning

Kandidatuppsats, 10 poäng, inom det systemvetenskapliga programmet

Omfång: 58 sidor

Handledare: Anders Svensson

Examinatorer: Mia Sassén
Erik Wallin

Abstrakt

I en värld full av teknik och information som flödar är det viktigt att ha kontroll över den data som anses vara viktig för organisationen. Skulle informationen hamna i orätta händer kan det innebära förödande konsekvenser för organisationen och i vissa fall även deras kunder. För att undvika detta bör rätt sorts skydd anpassas till den typ av data man avser att skydda men även organisationen som helhet. Aspekter som frekvens och förödelse vid ett hot men även hur viktig datan är, är olika aspekter som måste utvärderas för att kunna anpassa och investera i rätt typ av skydd. Denna studie jämför två svenska IT-relaterade företag i varierande storlekar med avsikten att undersöka om det finns en relation mellan datasäkerhetsmedvetandet och företagens storlek, eller om det finns en annan relation som påverkar graden av säkerhetsmedvetenhet i en organisation. De båda företagen är kopplade till utveckling och konsultverksamhet men inom olika områden. I studien ställer vi de båda företagen i relation till varandra och visar likheter och skillnader i deras datasäkerhetsarbete, både i deras egen organisation men även gentemot deras kunder.

Nyckelord

data, säkerhet, medvetenhet, jämföra, hot, skydd, policy

Tack

Vi vill tacka de personer som gjort att denna studie har kunnat genomföras och har valt att delta i de intervjuer vi anordnat och har ställt upp med sin dyrbara tid för att medverka och bidra med mycket värdefull information.

Vi vill även tacka vår handledare Anders Svensson som kritiserat, stöttat och guidat oss mot vårt slutresultat. Vi tackar även de grupper som har gett kritik på vår uppsats.

Innehållsförteckning

Figurförteckning

1. Inledning

Vår egna och omgivningens säkerhet är något som vi alla är måna om och viljan för att skapa hög säkerhet är stor. När det gäller ens fysiska säkerhet, pengar eller bostad. Vi vet alla att det är att föredra att gå på en upplyst gata istället för en mörk gränd, att inte ha alla sina besparingar i plånboken och att man låser sin ytterdörr när man ska på semester. Det är naturliga skyddsmekanismer som uppkommit genom både dina egna och andras erfarenheter i det ”verkliga livet”. Hur är det då i den virtuella världen där liknande hot finns som och ger liknande konsekvenser? Är du medveten om vilka hot du och din organisation står inför och hur ni skyddar er mot dessa på ett adekvat sätt?

1.1. Bakgrund

Enligt Wallström (2005) anmäls inte 20 procent av de brott som är relaterade till IT-säkerhet och han menar även att förekomsten av dataintrång och andra IT relaterade brott är förhållandevis vanlig och kan utsätta en organisation för stor skada. Enligt Pfleeger & Pfleeger (2003) kan datasäkerhet jämställas med en tillitsförsäkring. Pfleeger & Pfleeger (2003) menar även att skyddad information väcker ett visst intresse för att tränga genom de säkerhetslösningar som företagen i fråga använder sig av. Att veta vid vilket tillfälle och vilken typ av attack som är riktad mot en organisations data är omöjlig att förutse enligt Pfleeger & Pfleeger (2003). Det är först när attacken utförs som företaget får denna information. Under år 2006 anmäldes det enligt Brottsförebyggande rådet (2007) 849 fall av dataintrång i Sverige och mörkertalet av denna typ av brott anses vara stora.

Då dagens företag är beroende av IT (Knapp, Marshall, Rainer Jr och Morrow, 2006) anser Mitrović (2005) att företagen inte har råd med att bli skadade genom denna typ av attacker och rekommenderar att företagen ska säkra sin information, och att detta är ett långsiktigt arbete. Enligt Panko (2004) går det inte att välja en lösning ur en lista utan det är en lösning som anpassas efter organisationen och dess behov av skydd för en viss typ av data. Enligt Mitrović (2005) spelar det ingen roll i vilken form denna data befinner sig i, utan det är värdet på den data som man avser skydda som bestämmer hur datasäkerheten utformas.

Vi anser att detta är ett aktuellt område att undersöka då företagen idag är beroende av datorer för att klara av många av de arbetsuppgifter de ställs inför. Enligt Mitrović (2005), McCumber (2005) och Pfleeger & Pfleeger (2003) måste de tre säkerhetsbegreppen integritet, sekretess och tillgänglighet anpassas efter organisationen för att kunna tillhandahålla en relevant och tillförlitlig data i ett system till rätt personer. McCumber (2005, s. 174) menar att ”security is not simply something you implement and forget; it is a way of doing business”. För att kunna implementera och konfigurera de säkerhetslösningar man anser ska fungera i sin organisation måste man enligt McCumber (2005) ha kunskapen både om hoten och om dess konsekvenser. Vi anser att det är viktigt att undersöka i vilken grad datasäkerhetsmedvetenhet finns hos svenska företag i en värld där tekniken ständigt förändras.

1.2. Problemområde

Statistik från Statistiska Centralbyrån (SCB, Andel företag som använder datorer efter storleksklass och bransch, 2007) visar att 96 procent av de svenska företagen använder IT i någon bemärkelse. Statistiken visar att svenska företag förlitar sig mer och mer på IT de senaste åren och därmed är det av stor vikt att på bästa möjliga sätt skydda den information som lagras på företagens IT-medel. Statistiska Centralbyrån (SCB, Andel företag som använder olika säkerhetsanordningar, 2007) visar att företag de senaste åren har utökat sina säkerhetslösningar successivt. Vi anser att det är viktigt att ett företag ska ha god datasäkerhet och en medvetenhet om de hot och säkerhetslösningar som är mest lämpade för verksamheten, för att säkerställa att den mängd data som färdas och lagras över IT inte hamnar i fel händer. Vi vill med denna studie undersöka hur medvetna två svenska IT-företag är om datasäkerhet men också hur deras medvetenhet är relaterad till deras storlek. Vi anser att storleksskillnaden är viktig att belysa för att kunna besvara den frågeställning vi ställer inför denna studie men även för att kunna verifiera eller falsifiera vår hypotes där storleken har en stor betydelse. Vidare så anser vi att storleksskillnaden i företagen är betydelsefull på grund av att man får en inblick i hur medvetenheten speglas i ett litet företag i relation till ett stort företag.

1.3. Syfte

Vi avser att göra en värdering av hur datasäkerhetsmedvetna två svenska IT-relaterade företag är. Värderingen sker genom att jämföra företagen av olika storlekar i förhållande till varandra för att se eventuella skillnader och likheter, samt att relatera detta till relevant och aktuell forskning inom IT-säkerhet. Värderingen kan ligga till grund till fortsatt forskning inom området men även för att få en inblick av hur relationen mellan företagens storlek och datasäkerhetsmedvetenheten förhåller sig.

1.4. Frågeställning

Hur ser två svenska IT-företags datasäkerhetsmedvetenhet ut och hur skyddar de sig i förhållande till deras verksamhet och storlek?

1.5. Hypotes

Den hypotes vi kommer arbeta efter är att det finns en relation mellan företagens storlek och dess medvetenhet inom datasäkerhet. Det vill säga att ett större företag antas ha större medvetenhet angående datasäkerhet till skillnad från det mindre företaget vars medvetenhet antas vara närmare det sunda förnuftet. De stora skillnaderna mellan företagen antar vi kunna bero på aspekter så som ekonomiska resurser, erfarenheter, bemanning och respektive företags hotbild.

1.6. Målgrupp

Studien riktar sig till studenter, lärare, forskare samt svenska företag som har intresse för datasäkerhet och datasäkerhetsmedvetande. På grund av ämnets vida karaktär samt olika bredd i

intressenternas förkunskaper har vi valt att grundläggande beskriva de hot och skydd som finns samt beskriva datasäkerhet, policys och säkerhetsmodeller med hjälp av tidigare forskning. Kapitel 3 är därmed riktad till personer med ingen eller liten förkunskap i ämnet.

1.7. Avgränsningar

Studien avgränsas till att studera och jämföra datasäkerhetspolicys och datasäkerhetsmetoder mot både interna och externa hotbilder hos två svenska företag som är verksamma inom samma område och är av olika storlek.

1.8. Disposition

Kapitel 1 – Inledning
I detta kapitel ges en introduktion till problemområdet som är valt men även studiens syfte, frågeställningar och avgränsningar.

Kapitel 2 – Metod
I detta kapitel presenteras vår valda forskningsstrategi och metod. Kapitlet innefattar även tillvägagångssättet och tar upp termer som reliabilitet, validitet och replikerbarhet.

Kapitel 3 – Teoretiskt underlag
I detta kapitel presenteras de teorier som studien grundar sig på. Kapitlet är indelat i fem delar. Den första delen förklarar ett urval av relativa hot som finns mot data och del två tar upp olika skydd man använder sig av för att skapa en tryggare tillvaro. Den tredje delen förklarar begrepp som ligger till grund för en god datasäkerhet men även olika typer av datasäkerhet. Den fjärde delen beskriver vad en policy är och ger exempel på detta. Den sista delen beskriver vanliga säkerhetsmodeller och dess nytta i en organisation.

Kapitel 4 – Empirisk undersökning
I detta kapitel presenteras resultatet av de båda intervjuer som utförts.

Kapitel 5 – Analys
I detta kapitel ställs den empiriska undersökningen och dess intervjuer i relation till varandra och visar att det finns vissa likheter och skillnader mellan företagen. Vidare så analyserar vi företagens hotbild samt hur företagen arbetar för att upprätthålla datasäkerhet.

Kapitel 6 – Slutsats
I detta kapitel redovisas våra slutsatser och besvarar frågan på hur företag av olika storlek inom samma bransch står i relation till datasäkerhetsmedvetenhet. Även självkritik på studien och förslag på fortsatt forskning presenteras.

2. Metod

2.1. Val av forskningsstrategi

Bryman (2002) beskriver två olika forskningsstrategier, den kvalitativa och den kvantitativa. Denna rapport kommer att vara induktiv, tolkande och resultatet publiceras med ord istället för siffror och detta stämmer väl överens med den kvalitativa forskningsstrategin som vi väljer att arbeta efter. Backman (1998) beskriver tre framträdande grundbegrepp inom den kvalitativa forskningen som innebörd, kontext och process. Detta betyder att forskaren intresserar sig för individer som upplever, tolkar och strukturerar i relation till sina tidigare upplevelser och erfarenheter i ”real-life”-situationer.

2.2. Metodval

2.2.1. Litteraturgranskning

Studien grundar sig framför allt på teori inom områdena datasäkerhet, datasäkerhetspolicys och datasäkerhetsmetoder. Bryman (2002) anser att det är av stor vikt att man som forskare bör inta ett kritiskt förhållandesätt till litteraturen och med detta som grund har vi med bästa möjliga medel försökt analysera, tolka och kritisera litteraturen som valts ut för studien. Backman (1998) menar att forskaren utgör instrumentet i studien och kan inkorporera stereotyper, fördomar eller förutfattade meningar i ett område vilket kan leda till att nya upptäckter förbises eller inte noteras. Backman (1998) menar att det finns olika uppfattningar om hur detta moment ska utföras, en av dessa uppfattningar är att det ska finnas en måttlig och orienterad beläsenhet i området och vi har valt att följa detta råd.

Backman (1998) benämner flera funktioner som litteraturgranskningsmomentet ska ge och vi har valt ut de funktioner som vi anser är av vikt för vår studie:

- Ge en översikt och orientering över tidigare samlad kunskap inom området
- Indikera problem
- Visa betydelsen, hjälpa och precisera problemformulering
- Ge teorier inom områdena datasäkerhetspolicys och datasäkerhetsmetoder

2.2.2 Intervjuer

Enligt Bryman (2002) finns det flera olika sätt att utföra en intervju på men vi har valt att följa ett semistrukturerat intervjuförfarande då vi anser att detta tillvägagångssätt är mer strukturerat och passar oss bättre än det ostrukturerade intervjuförfarandet. Vidare menar Bryman (2002) att det semistrukturerade intervjuförfarandet följer en intervjuguide som innehåller de ämnen och punkter man vill beröra i intervjun. Frågorna behöver inte ställas i samma ordning som är angivet

i intervjuguiden och ytterligare frågor får tillkomma under intervjuns gång. Enligt Bryman (2002) gör detta att intervjun blir mer interaktiv men inte lika lik ett samtal som den ostrukturerade intervjun. En nackdel enligt Bryman (2002) med det semistrukturerade intervjuförfarandet är att frågorna kan bli svåra att jämföra med andra intervjuer.

2.3. Undersökningens genomförande

2.3.1. Val av deltagare

Urval i den kvalitativa forskningsstrategin är respondenter vars syfte är att ge ökad förståelse och insikt (Backman, 1998). Vårt urval av respondenter består av personer, anställda på olika svenska IT-relaterade företag i olika storlekar, vars arbetsuppgifter berör ämnet datasäkerhet och har en markerad syn på detta. Då vi har valt att göra en komparativ studie anser vi att antalet informationskällor, i detta fall respondenter från två svenska IT-relaterade företag, måste vara två eller flera.

Vi valde att antalet respondenter skulle uppgå till två stycken och att de skulle vara IT-relaterade för att därmed ha något gemensamt. Många företag valde att tacka nej på grund av att de ansåg att de inte hade en direkt säkerhetsfilosofi eller markerad syn på datasäkerhet och ansåg sig därför inte det lämpligt att medverka. Andra företag valde att tacka nej på grund av tidbrist eller bristande intresse. För att kunna uppnå det bestämda antalet respondenter var vi tvungna att tillfråga relativt många företag. Företagens anledningar att inte vilja medverka kan till stor del vara sanna, men vi tror att avvisandet grundar sig till stor del i ämnets känsliga natur.

Till slut fick vi två företag som accepterade och därmed intervjuades. Atea i Sverige är ett stort företag som existerar i hela norden men under olika namn. De utvecklar IT-infrastrukturlösningar åt företag och organisationer. MOROTSmedia och är ett mindre systemutvecklingsföretag lokaliserat i forskningsbyn IDEON i Lund. Respondenten på Atea i Sverige önskade att vara anonym och kommer därför inte benämnas vid namn utan med titeln konsult till skillnad från respondenten på MOROTSmedia som benämns med namn.

2.3.2. Tillvägagångssätt vid intervjuer

Tiderna för de båda intervjuerna bokades över telefon och en timme blev avsatt för att kunna utföra intervjun. Innan intervjun blev respondenterna underrättade om ämnet och syftet med intervjun och fick även intervjufrågorna skickade till sig för att kunna förbereda sig om så behövdes. Intervjufrågorna skickades för att skapa tillförlitlighet, god etisk hållning till företagen samt för att ge respondenterna tid att förbereda sig och därmed ge mer ingående svar på relativt komplexa frågor. Intervjuerna ägde rum i respondentens konferenslokal för att få en avskärmad miljö utan störningsmoment men även för att skapa en trygghet hos respondenten.

Frågorna var i förhand bestämda, enligt Bilaga A, och frågorna blev inte ställda i angiven ordning utan blev utvalda i den ordning som passade intervjuns karaktär och ordning. Detta tillvägagångssätt är karaktäristiskt för den semistrukturerade intervjutypen (Bryman, 2002). Frågor som var intressanta eller otydligt besvarade följdes upp med nya improviserade frågor.

Hela intervjun spelades in med en digital diktafon för att vi senare skulle kunna återge hela intervjun på ett så korrekt och precist sätt som möjligt. Intervjun sammanfattades och denna text skickades till respondenterna för ett godkännande, dels för att upprätthålla en god validitet i det ihopsamlade materialet men även för att hålla god etik gentemot respondenten och dess företag (Bilaga D & E). Respondenten fick kommentera och ändra den text som denna ansåg att vi missförstått. De kommentarer som respondenten gav har vi sedan utvärderat och skrivit till i sammanfattningen av intervjun.

2.4. Undersökningskvalitet

2.4.1. Värderingar

I nutidens forskningsvärld är det svårt att utföra en studie utan att ha förutfattade meningar då dessa är starkt kopplade till varje individs värderingar. ”Värderingar kan dyka upp när som helst i en undersökning” enligt Bryman (2002, s. 37). De olika faserna i forskningsprocessen påverkas av forskarnas värderingar och resulterar i en mer eller mindre styrd studie. (Bryman, 2002)

Självklart fanns det värderingar i vår studie som gjorde att vi valde just detta ämne, de har påverkat vårt val av intervjuföretag, våra slutsatser, o.s.v. De värderingar som fanns innan studien påbörjades var att storleken på IT-företagen skulle på något sätt bestämma företagets datasäkerhetsmedvetenhet. De större företagen skulle ha total kontroll på sin teknik medan de mindre företagen skulle använda sig av sunt förnuft för att upprätthålla en datasäkerhet proportionell till företagets storlek.

2.4.2. Reliabilitet, validitet och replikerbarhet

Reliabilitet är enligt Bryman (2002) ett mått på studiens styrka i avseendet att kunna utföra en ny undersökning och ändå få samma resultat eller om resultatet beror på slumpmässiga eller tillfälliga egenskaper. För att denna studie ska erhålla en förstärkt reliabilitet har vi valt att bifoga de intervjufrågor vi använt oss av (Bilaga A) tillsammans med de transkriberade intervjuerna (Bilaga B & C). Detta gör att man ser vilka frågor som ställts vid intervjuerna inklusive svaren och dess följdfrågor.

Validitet är ett annat kriterie vid bedömning av en studie och avser att kontrollera eller bedöma hur väl studiens slutsatser är relaterade till övrig publicerad information i studien (Bryman, 2002). Vi anser att de slutsatser som är publicerade i vår studie är väl förankrad till den information som visas i den teoretiska genomgången. Bryman (2002) beskriver även extern validitet som fungerar som ett delmått i validitetsmätningen och mäter hur väl resultaten kan generaliseras och appliceras på andra undersökningsområden. Efter analysen av vårt resultat bildade vi oss en annan uppfattning kring relationen mellan säkerhetsmedvetenhet och företagets storlek. Vi anser att resultatet i vår studie kan generaliseras om man tar hänsyn till den teknikkompetens och det teknikkrav som företagen har istället för att se till företagets storlek.

Vi anser att replikerbarheten i denna studie är relativt enkel då två företag intervjuades och ställdes i relation till varandra. Precis som Bryman (2002) menar är replikerbarhet ett mått på hur väl andra forskare kan reproducera både undersökning och resultat. Då företagens intresseområde är fokuserade på IT tror vi att fortsatta studier kommer att styrka vårt resultat.

3. Teoretiskt underlag

3.1. Hot

3.1.1. Vad är hot?

McCumber (2005) menar att ett hot kan vara en person, en händelse eller en viss situation som öppnar dörrar och möjligheter för att skada eller dra nytta av någon annans tillgångar. Vidare menar McCumber (2005) att företag försöker minska denna hotbild genom att undervisa anställda, införa diverse processer och olika konsekvenser för att förhindra och avskräcka de personer som försöker ta del av, förändra eller påverka ett företags tillgångar. Enligt Mitrović (2005), Pastore & Dulaney (2006) och McCumber (2005) delas hoten in i fysiska, logiska och mänskliga/organisatoriska hot och framställs i en vision av en hotbild genom analys av hot, svagheter och sårbarheter i organisationen och dess system.

McCumber (2005) kategoriserar de olika hoten i två olika gruppar där mänskliga hot är en del och ickemänskliga hot är en annan. De mänskliga hoten kategoriseras upp i interna och externa hot där man ser om hotet uppkommer inom organisationen (insider) eller från någon utanför. De mänskliga hoten kan enligt Mitrović (2005) uppstå vid otydlig ansvarsfördelning och vid felaktiga eller bristande tilldelningar av behörigheter i systemet. Det är därför viktigt att utforma en säkerhetspolicy som tydligt beskriver hur man ska hantera sådana här situationer. McCumber (2005) beskriver de interna hoten som antingen ofientliga eller fientliga då de fientliga hoten kan medvetet ställa till problem för organisationen på olika sätt – strukturerat eller ostrukturerat. McCumber (2005) ger ett exempel på ett ofientligt och ostrukturerat hot som är misstag och andra fel som kan uppstå vid användandet av ett system. För att minska denna typ av hot förelår Mitrović (2005) att man som nyanställd ska få en ordentlig utbildning i de system man förväntas använda men även tydliga instruktioner på vilka arbetsuppgifter som man ska utföra och vilka befogenheter man har. Mitrović (2005) menar att en loggningsfunktion är en viktig del i att bekämpa denna typ av hot, och tillsammans med en god behörighetsadministration har man möjligheten att spåra och bevisa otillåten aktivitet inom organisationen. Mitrović (2005) beskriver det ickemänskliga hotet som ett fysiskt hot. Denna typ av hot innefattar skador eller stöld av saker man kan se såsom hårddiskar, minnen, processorer, fläktar och andra komponenter som ingår i en datorlösning. Även oväntade väderförhållanden såsom åska, översvämning och brand räknas in i den kategori som Mitrović (2005) beskriver ovan.

3.1.2. Vilka hot

Stallings (2002), Pfleeger & Pfleeger (2003) och Panko (2004) menar att hackers är ett fenomen i dagens informationssamhälle och dessa personer är kunniga i programmering och elektroniska intrång. De menar också att de personer som vill göra intrång i system gör detta för att få mer respekt eller för egen vinning och tar sig därmed in i ett system eller en server för att stjäla eller förstöra viktig data eller information.

Stallings (2002) och Pastore & Dulaney (2006) menar att virus är den mest sofistikerade typen av hot mot datorsystem på grund av dess natur att utnyttja de sårbarheter som finns tillgängliga hos systemet. Stallings (2002) och Pastore & Dulaney (2006) definierar ett virus som ett program vars syfte liknar ett biologiskt virus eller en parasit då de infekterar andra program genom att förändra dem. Ett datorvirus försöker inbädda ett program och därefter smitta andra program genom att göra perfekta kopior av sig själv som bäddar in sig i programmen. Stallings (2002) och Pastore & Dulaney (2006) förklarar att maskar har ett snarlikt beteende och liknar på många sätt virus men behöver dock inte en medveten person för att sprida sig vidare. En mask söker aktivt efter andra maskiner för att sedan infektera dem med till exempel ett virus eller en trojansk häst. Stallings (2002) och Pastore & Dulaney (2006) förklarar att trojanska hästar är farliga förklädda program. De ser vanligtvis ut som något harmlöst program men de exekverar oönskad och skadlig programkod.

Utöver hacking, virus och andra hot, som förklaras ovan, så framför Stallings (2002) att det finns hot som pornogafi, e-post som är sexuellt eller etniskt trakasserande, samt oönskade email i form av spam. Stallings (2002) menar att dessa typer av hot är skadliga i den bemärkelsen att de tar upp resurser i form av tid samt att de kan beröra personer illa inom företaget och detta är givetvis något som företag vill förhindra och minimera.

3.2. Skydd

3.2.1. Behörighet

En effektiv behörighetsadministration är enligt Mitrović (2005) A och O och han anser att denna är nyckeln till en god IT-säkerhet. Ett normalstort företag har oftast många ställen där lösenord krävs för att komma åt den data som är skyddad. Enligt Mitrović (2005) kan dessa ställen uppgå i 100-tal i vissa företag och det innebär att vid nyanställning eller vid förändrade behörigheter för en anställd måste behörighetsinformationen läggas till, alternativt uppdateras, på samtliga ställen de anställda måste logga in på för att få den rätta behörigheten. Ytterligare en dimension kan läggas till enligt Mitrović (2005) då många företag arbetar mot externa datakällor och behörighetskontrollen står inför nya utmaningar. Att ha kontroll på de aktiva användarna och på de konton som är inaktiva på grund av avslutad anställning eller annan anledning kan vara svår enligt Mitrović (2005). Pastore & Dulaney (2006) belyser svårigheterna med kontrollen av att obehöriga inte får åtkomst till företagets data eller resurser ovanpå detta. Pastore & Dulaney (2006) menar att om detta ska fungera effektivt behöver lösningarna anpassas till organisationens säkerhetsfilosofi. Pastore & Dulaney (2006) menar även att olika personer har olika behörigheter till den lagrade datan och detta specificeras oftast i en säkerhetspolicy, som beskrivs senare i vår studie.

3.2.2. Lösenord

Stallings (2003) menar att lösenord är det främsta skyddet mot intrång då ett lösenord används för att verifiera ett användarnamn på ett system. Precis som på ett vanligt kombinationslås så är det viktigt att välja en kombination som inte är lätt att gissa för att motverka intrång. Panko (2003) anser att en användare med ett svagt lösenord, det vill säga ett kort lösenord som endast använder bokstäver och som är ett vanligt ord, skapar en väg till för intrång mot servern. Då en användare har ett lösenord som endast består av bokstäver, där lösenordets längd är N bokstäver

långt, skulle det alltså ta 26^N försök att hitta rätt lösenord. Stallings (2003) menar att det därför är mycket viktigt att använda starka lösenord och att systemet inte tillåter oändliga antal försök för att skriva in lösenordet. Det följande är enligt Stallings (2003) karaktäristiska egenskaper för ett starkt lösenord:

- Lösenordslängd på minst 8 tecken
- Minst en versal- och gemenförändring
- Lösenordet måste innehålla minst en siffra som inte är i slutet av lösenordet
- Samt att lösenordet måste innehålla ett tecken som varken är en bokstav eller en siffra som till exempel #.

3.2.3. Säkerhetskopior

Både Mitrović (2005) och Panko (2004) anser att då datalagring oftast sker på en hårddisk och denna har en begränsad livstid är det viktigt att säkerhetskopiera viktig data. Enligt Mitrović (2005) och Panko (2004) är den information som bör säkerhetskopieras är den typ av information som är omöjlig eller svår att återskapa på annat sätt. Mitrović (2005) och Panko (2004) påpekar att det finns olika sätt att utföra en säkerhetskopiering på och i samtliga fall är det att rekommendera att säkerställa att säkerhetskopian verkligen fungerar. Pastore & Dulaney (2006) menar att andra anledningar till att säkerhetskopieringar bör utföras är p.g.a. naturkatastrofer, fysiska attacker, virusangrepp eller programvarufel.

3.2.4. Brandväggar

Brandväggar är numera något som förekommer i nästintill varje svenskt hem och företag som har datorer och nätverk. En brandvägg sitter vanligtvis mellan Internet och ett nätverk där dess uppgift är att skydda nätverket och dess datorer men även utåt från det egna nätverket . Brandväggar kan beskrivas som grindvakter som släpper in det som är välkommet men håller ute det som inte är det. Panko (2003) förklarar en brandväggs arbete som ett filter då de godkänner eller nekar de paket som skickas till och från nätverket. Vidare menar Panko (2003) att brandväggar är ett utmärkt skydd mot hacking, DoS attacker och dylika hot.

3.2.5. Antivirus

Stallings (2002) menar att det idealiska skyddet mot virus är att hindra fäste i arbetsstationer och nätverk. Att förhindra fästet är enligt Stallings (2002) generellt omöjligt men man kan reducera virusattackerna markant. Stallings (2002) menar att det bästa alternativet efter förhindring är ett antivirussystem då dessa fungerar genom detektion, identifikation samt borttagning. Panko (2003) anser att de tidiga versionerna av antivirus endast fungerade som skanners där man sökte efter befintliga virus i datorn. Enligt Panko (2003) är de flesta antivirus på marknaden nu fjärde generations antivirussystem som är ett helt paket av olika antivirustekniker. Dessa tekniker, så som skanners och aktivitetsfällor, arbetar tillsammans för att förhindra att virus får fäste i systemet samt att ta bort virus och återställa systemet om så skulle behövas.

3.2.6. Kryptering

Pfleeger & Pfleeger (2003), Pastore & Dulaney (2006), Panko (2003) och Stallings (2002) menar att kryptering är en metod för att skydda meddelande genom att förvandla meddelandet till bitar av strängar som endast kan dekrypteras och därefter läsas av mottagare. Originalmeddelandet kallas klartext och det krypterade meddelandet kallas skiffertext. Vidare beskriver de att en krypteringsmetod är en matematisk algoritm som krypterar klartext och dekrypterar skiffertext. Pfleeger & Pfleeger (2003), Pastore & Dulaney (2006), Panko (2003) och Stallings (2002) förklarar att den matematiska algoritmen utför olika ersättningar och förändringar av originaltexten för att göra den oförståelig. För att säkerställa att det endast är mottagaren som kan läsa det krypterade meddelandet beskriver Pfleeger & Pfleeger (2003), Pastore & Dulaney (2006), Panko (2003) och Stallings (2002) att det krävs en nyckel. Nyckeln är en sträng av bitar som tillsammans med krypteringsmetoden återskapar skiffertext till klartext.

Panko (2003) menar att symmetrisk nyckelkryptering är en metod där båda parterna använder samma nyckel. När ett meddelande krypteras med en nyckel så måste mottagaren ha denna nyckel för att kunna dekryptera meddelandet. Panko (2003) beskriver att det finns många olika populära symmetriska nyckelkrypteringsmetoder. Panko (2003) menar att den populäraste är Data Encryption Standard (DES). DES använder en nyckellängd på 56 bitar vilket är relativt svagt, dock finns det varianter på metoden där nyckeln använder fler antal bitar.

Panko (2003) förklarar att publik nyckelkryptering är en annan krypteringsmetod där varje part har sin egna privata nyckel. Utöver den privata nyckeln så har de också en publik nyckel som alla parter har gemensamt. Panko (2003) beskriver att istället för att ha samma nyckel så krypterar man meddelandet med mottagarens publika nyckel och mottagaren dekrypterar meddelandet med sin privata nyckel. Sändaren av meddelandet kan alltså inte dekryptera meddelandet efter det har krypterats.

3.3. Datasäkerhet

Datasäkerhet, eller informationssäkerhet som Mitrović (2005) väljer att beskriva termen, är det inom säkerhetsområdet allmänt känt att datasäkerhet är uppbyggt utav tre olika element som skapar den säkerhet man eftersträvar – sekretess, integritet och tillgänglighet. McCumber (2005) menar att datasäkerhet är kontextberoende då datasäkerhet är beroende på hur den aktuella verksamheten ser ut och vilka krav man har på säkerhet eller om uppbyggnaden och relationen mellan grundtermerna ser olika ut. McCumber (2005) menar även att datasäkerhetslösningarna varierar beroende hur den aktuella verksamheten ser ut. McCumber (2005) påpekar att det finns vissa frågor som en datasäkerhetsansvarig måste veta svaret på innan arbetet mot en säkerhetslösning kan påbörjas. Dessa frågor ger riktlinjer och tillsammans ger de en god grund för en datasäkerhetspolicy. Det kan vara frågor som berör skador som kan uppkomma, hur lätt det ska vara att komma in i nätverket, internt eller extern, eller frågor som rör den ekonomiska aspekten. Hur mycket ska vi skydda? För vilka? Hur mycket pengar ska vi satsa för att kunna upprätthålla detta? Detta är några av de frågor som McCumber (2005) förespråkar. Enligt Mitrović (2005) handlar god datasäkerhet till 80 procent om människor och processer och till 20 procent om teknik.

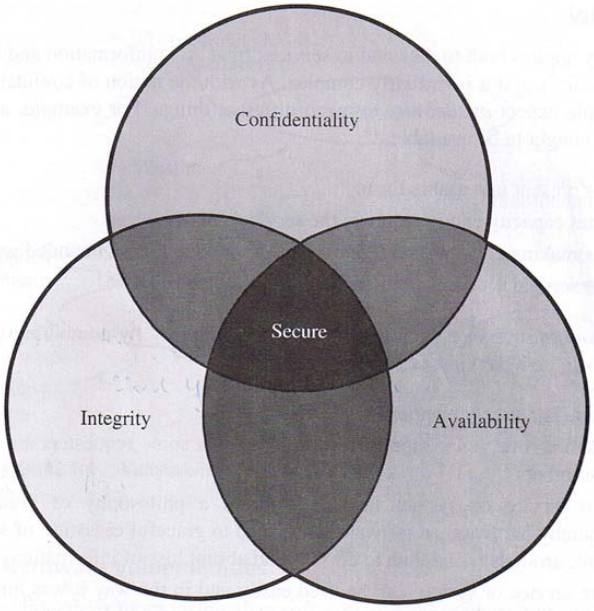
Davies (2006) menar att virus framställs som det stora datasäkerhetshotet men så inte är fallet. Enligt Davies (2006) är det farligaste hotet att förlora den viktiga data som man avser att skydda och särskilt utsatt är de portabla lagringsenheterna som lätt kan försvinna eller stjälas. Davies

(2006) menar att möjligheterna och situationerna är många för hur en sådan enhet kan komma i fel händer och lösningen på denna typen av problem är att sätta ett lösenord på den data som avses att skyddas. Lösenord kan tolkas på flera sätt och kan vara en bokstavskombination eller andra identifikationslösningar. Davies (2006) framför olika sätt som kan säkerställa åtkomst till en skyddad data så som fingeravtryck, röstigenkänning eller näthinnescanning på ögat.

Bernard (2007) menar att data kan existera i olika former och lagras därmed på olika sätt för att tillmötesgå det aktuella mediet. Oavsett hur informationen är lagrad bör den skyddas på ett tillfredsställande sätt och det innebär att man skyddar informationen mot flertalet hot för att minimera riskerna och maximera inkomsten av gjorda investeringar men även för att skapa nya möjligheter.

3.3.1. Sekretess, integritet och tillgänglighet

Mitrović (2005), Panko (2004) och Pfleeger & Pfleeger (2003) menar att säkerhet är uppbyggt av tre termer; sekretess (confidentiality), integritet (integrity) och tillgänglighet (availability) och tillsammans skapar de en unik kombination för säkerhet i en specifik kontext (se Figur 1). Dessa tre termer är enligt Mitrović (2005) till för att skapa riktlinjer, policies och förhållningssätt för organisationen i närheten av den data man är rädd om.



Figur 1: Sekretess (confidentiality), integritet (integrity) och tillgänglighet (availability) (Pfleeger & Pfleeger, 2003, s. 11)

Sekretess: Pfleeger & Pfleeger (2003) menar att sekretess försäkrar att endast behöriga personer kan läsa, se, skriva ut men även att vetskapen att denna information överhuvudtaget finns ska vara begränsad till en viss utvald grupp av användare. Sekretessen är mer förståelig än de andra två termerna för att det är enkelt att koppla liknande exempel med samma innebörd i det verkliga livet. McCumber (2005) menar att sekretessen är den term som är mest studerad men inte med anledning av att den är kopplad till säkerhetsfrågor utan för att kunna förstå och förbättra möjligheten att rätt person får reda på rätt information och ingen annan. Redan under romartiden började man tävla om vilken som kunde skicka meddelanden som endast berörda parter kunde läsa och med tiden har denna teknik blivit extremt komplex men dock finns gemensamma lösningar. McCumber (2005) menar att dagens kryptologiska lösningar har liknande delstrukturer

som förr då man fortfarande använder en algoritm och en förbestämd nyckel. Beroende på hur komplext system och hur många olika användare som inkluderas i lösningen kan denna policyskapande processen variera mellan relativt enkel och extremt komplex. McCumber (2005) beskriver sekretess som ett enkelt koncept som i verkligheten behöver ett del teknologi och ett anpassat IS, men när en säkerhetspolicy väl är utvecklad har man grunden för att kunna bestämma kraven för kryptografin och andra sekretessprocesser.

Integritet: Pfleeger & Pfleeger (2003) menar att det finns många olika benämningar på integritet beroende på vilken kontext man befinner sig i och några av dessa betydelser finns även representerade i den riktiga världen medan andra finns i datorvärlden. Några betydelser som beskrivs är; exakt, noggrann, oförändrad, modifierad av auktoriserade personer, överensstämmande eller meningsfull. McCumber (2005) menar att integriteten i säkerhetsaspekten är en grundläggande faktor och menar också att det finns olika betydelser i olika kontexter. Gemensamt för Pfleeger & Pfleeger (2003) och McCumber (2005) är att oprecis information kan vara värdelös om integriteten av denna inte kan hållas på den nivå som är ställd till organisationen. Vidare menar de att den definition som är mest accepterad och använd är att dataintegritet är när man är försäkrad att informationen bara kan visas för och modifieras av behöriga användare, men denna definition kan vara lite missvisande då den antar att alla behöriga användare modifierar all data med 100 procents tillförlitlighet vilket inte alltid stämmer.

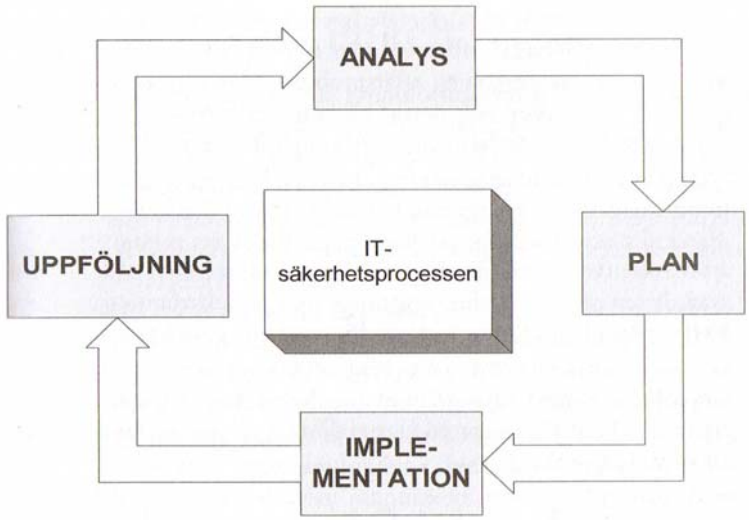
Tillgänglighet: McCumber (2005) menar att information som inte finns, är inte tillgänglig. Detta betyder att informationen ska vara tillgänglig när den behövs och sträcker sig i tiden mot oändlighet. Denna term och tillika egenskap ur ett datasäkerhetsperspektiv är lika viktig att analysera och observera som de andra två egenskaperna för att få en lösning som passar de mål och förväntningar man har på sitt system. Enligt McCumber (2005) finns det två aspekter man kan ta del av för att skapa en tillförlitlig tillgänglighet – redundans och säkerhetskopiering eller återställning. Att ha redundans i bland annat databaser och nätverk kan enligt McCumber (2005) kosta lite extra då hårdvara och underhåll är dyrare, men detta ska då vägas mot konsekvenserna av otillgänglighet. En säkerhetskopiering är en kopia av data som kan vara känslig att förlora på grund av dataförlust eller applikationsfel. Denna backup kan vid behov återställas för att kunna återgå till normalt arbete. Pfleeger & Pfleeger (2003) beskriver även att diverse tjänster inkluderas i tillgänglighetsprincipen och om data och tjänster kan publiceras i en användbar form, att kapaciteten är tillräckligt stor för en viss service och även att tjänsten är slutförd inom rimlig tid.

3.3.2. Människa, teknik och process

Mitrović (2005) framför ett ramverk som frambringar den goda IT-säkerhet som en säkerhetsmedveten organisation efterfrågar. God informationssäkerhet består av tre olika delar - människa, teknik och process – där människan utgör grunden för en lyckad säkerhetslösning. Mitrović (2005) menar att de övriga två elementen teknik och process är lättare att hantera programmatiskt och systematiskt när problem uppstår, men även genom att förhindra sådana problem. På grund av att människan är en så stor del i detta ramverk och tillika säkerhetslösning beror många beslut på hur människan är i sinnet vid beslutsfattandetillfället. Mitrović (2005) menar att besluten kan påverkas av yttre faktorer men även människans psykiska hälsa och den erfarenhet som människan har, och som kan tränas upp med hjälp av experimenterande och lära sig av sina egna misstag.

Mitrović (2005) beskriver säkerhetsprocessen som en iterativ handling där fyra underliggande aktiviteter finns – analys, plan, implementation och uppföljning (se Figur 2). Analysen besvarar vad och mot vad/vilka detta ska säkras och svaren på dessa frågor ska finnas i organisationens

datasäkerhetspolicy. Finns ingen datasäkerhetspolicy är det första steget att skapa en sådan. För att kunna göra detta anser Mitrović (2005) att man behöver en god vetskap av den hotbild som finns mot organisationen och denna framkommer i samband med att analysera och finna hot, svagheter och sårbarheter i IT-lösningen som man vill skydda. Mitrović (2005) menar att man behöver ha en plan över implementationen för att kunna realisera en god datasäkerhetslösning mot resultat som genererats fram i analysfasen. Denna ska innehålla aktiviteter, investeringar och tidsuppskattningar för dessa. För att kunna lära av sina misstag och säkerställa god kvalitet på en utvecklad datasäkerhetslösning måste denna utvärderas och denna utvärdering ligger till grund för nästkommande analysfas då hela säkerhetsprocessfasen är iterativ.



Figur 2: Säkerhetsprocess (Mitrović, 2005, s. 53)

Mitrović (2005) menar att den sista delen som frambringar god IT-säkerhet är teknik och denna utvecklas ständigt och därför behöver även organisationernas datasäkerhetsansvariga personer följa med i denna teknikutveckling. Mitrović (2005) menar att standarder, hot och skydd är några av de områden som ständigt förändras som man som datasäkerhetsansvarig måste ha god kunskap inom. Mitrović (2005) menar att ett system eller IT-lösning som utvecklats för 10 år sedan hade inte samma hotbild eller samma tekniska lösningar som finns i de system som utvecklas idag och därför är det även här viktigt att skapa en säkerhetslösning som kan anpassas även till de äldre IT-systemen genom att ersätta eller vidareutveckla de produkter man har i dagsläget. Den ultimata lösnigen enligt Mitrović (2005) är att kunna definiera vem som gör vad och sedan säkerställa genom uppföljning att så sker även i fortsättningen.

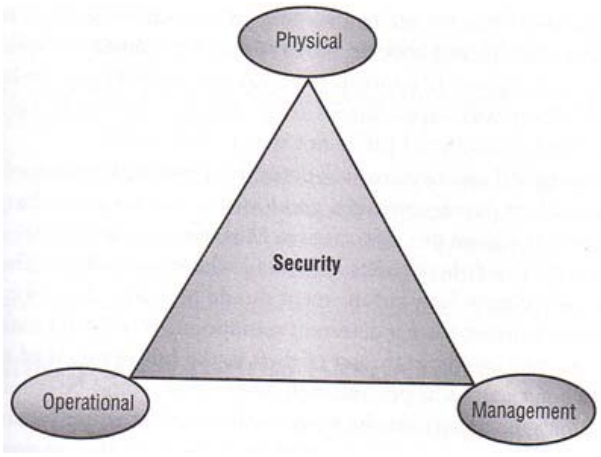
3.3.3. Typer av säkerhet

Enligt Bernard (2007) har flera organisationer de senaste decennierna lagrat sin information på fysiska medier så som papper och annat liknande. Enligt Bernard (2007) finns det ett flertal modeller som påvisar hur data bör hanteras och de nyare modellerna visar ett klart stöd för den elektroniska data som lagras i organisationerna. Enligt Bernard (2007) bevisar detta att data migrerar från det fysiska lagringsmediet till det elektroniska mediet. Bernard (2007) menar även att den fysiskt lagrade informationen bör inkluderas på samma sätt som elektroniskt lagrad information inkluderas i säkerhetsplaneringen. Bernard (2007) beskriver att många företag i dagsläget har säkerhetslösningar nästan endast för den elektroniskt lagrade informationen även om mycket viktig information fortfarande finns i den fysiska formen. Scheraga (2006) beskriver att det är inte bara när företaget har den fysiska datan i sina ägor som det är viktigt att skydda

denna. Även efter det att det fysiska mediet är förbrukat och slängs kan man som företag fortfarande bli utsatt för datastöld då informationen fortfarande går att utläsa från det fysiska mediet.

Panko (2004) menar att företagen inte ska behöva betala pengar för en typ av säkerhet som inte är nödvändig då detta är slöseri med pengar och att man som organisation måste finna en passande säkerhetslösning med skydd mot rätt angrepp. Att skapa säkerhet som är anpassad till den specifika organisationen görs enligt Panko (2004) genom att finna lösningar mot de olika riskerna som man kan utsättas för och eftersom varje organisation utsätts för olika risker i olika prioriteringsgrader ser också säkerhetslösningarna olika ut då dessa är proportionella med riskerna. Kilcourse (2005, s. 47) menar att "It should be the responsibility of the donor of the shared information assets to define their use, and that will require the custodians of those assets to rethink the technical architectures that maintain them". Jones (2007) beskriver olika tillvägagångssätt och frågeställningar som man kan använda sig av samt för att ligga till grund när organisationen ska prioritera motaktioner mot säkerhetshoten både genom en förändring och för att kunna bibehålla önskade egenskaper kring sekretess, integritet och tillgänglighet. Panko (2004) menar att en organisation bör ha policys som beskriver hur personer inom organisationen bör arbeta och bete sig när de arbetar med skyddad information. En komplett och genomtänkt policy är ett måste då hackers letar efter svagheter i organisationen och de finns på de områden där ingen välutformad datasäkerhetspolicy finns definierad.

Pastore & Dulaney (2006) anser att olika saker som ska skyddas har olika behov av säkerhet och detta på olika sätt beroende på den aktuella organisationen. Begreppet säkerhet smalnas ner till informationssäkerhet och denna säkerhet byggs upp av tre säkerhetstermer som tillsammans skapar den totala informationssäkerhet som organisationen eftersträvar (se Figur 3). Ett grundbegrepp är fysisk säkerhet och detta innebär att man skyddar sina tillgångar mot fysisk åverkan. Mitrović (2005) menar att det spelar ingen roll hur bra logiskt skydd man har om man inte skyddar sin utrustning på det fysiska sättet också. Inpasseringssystem, larm, galler, placering av utrustning och UPS (Uninterruptible Power Supply) kan vara några lösningar för att skapa denna typ av säkerhet. Pfleeger & Pfleeger (2003) beskriver även vikten av fysisk säkerhet men då man oftast kan uppnå denna typ av säkerhet genom sunt förnuft. Naturkatastrofer och vandaler läggs även till på listan över fysiska hot. Pastore & Dulaney (2006) menar att denna typ av säkerhet är relativt enkel att uppnå men belyser även vikten av kännedom av vad som försvunnit/skadats och eventuellt av vilken eller vilka personer som utfört detta hot. Det andra grundbegreppet som framförs av Pastore & Dulaney (2006) är den operativa säkerheten där man kontrollerar hur organisationen utför det den utför. Här kontrollerar man säkerheten i nätverket och hur väl de policys som finns definierade fungerar. Bernard (2007) och Kilcourse (2005) menar att det finns typer av data som är svåra att skydda och det är ägarens ansvar att skydda denna då de är de enda personerna som kan göra detta. Exempel på sådan data är telefonböcker, information sparad i mobiltelefoner eller PDAs (Personal Digital Assistant). I det sista säkerhetsbegreppet som Pastore & Dulaney (2006) beskriver är organisationens ledning samt policyhantering, där man tillhandahåller organisationen med rutiner och riktlinjer, då det måste finnas ett samspel mellan dessa två element för att organisationen i sin helhet ska acceptera och efterfölja de regler och riktlinjer som skapas.



Figur 3: Informationssäkerhet (Pastore & Dulaney, 2006, s. 5)

Infrastrukturssäkerhet är också en typ av säkerhet som Pastore & Dulaney (2006) beskriver och det innebär att man har kontroll över bland annat organisationens nätverk, nätverksutrustning, servrar och arbetsstationer. En liknelse görs med en stad som innehåller vägar, motorvägar, omfartsleder och så vidare. Pastore & Dulaney (2006) menar att utvärdering av både hårdvara och mjukvara ingår i denna typ av säkerhetsanalys och genom att förändra en liten del i denna konstruktion kan det påverka andra delar och dessa konsekvenser måste analyseras tillsammans med konstruktionens hållbarhet som helhet.

3.3.4. Säkerhetsplanering och riskanalys

Pfleeger & Pfleeger (2003) menar att alla organisationer som arbetar med datorer som hanterar värdefull data ska ha en säkerhetsplan. En plan som beskriver hur datasäkerhetshot ska hanteras och eftersom tekniken förändras gäller planen en viss period och bör justeras efterhand då teknikutvecklingen förändras. Att säkerhetsplanera innebär enligt Pfleeger & Pfleeger (2003) att man har en beskrivning av organisationens situation i nuläget samt en plan för hur man tänker förbättra denna situation. Pfleeger & Pfleeger (2003) anser att datasäkerhetsplanen ska innehålla ett flertal punkter däribland policy, nuvarande situation, krav och tidsaspekter. Detta är bara några av de punkter som beskrivs och vägen till en komplett eller uppdaterad säkerhetsplan varierar stort. Pfleeger & Pfleeger (2003) anser att de personer som deltar i denna framtagningsprocess av säkerhetsplanen är personer med olika kopplingar till verksamheten och den värdefulla information som denna hanterar, oftast numera med hjälp av informationssystem. Pfleeger & Pfleeger (2003) menar att personerna kan ha hårdvarukompetens, vara administratörer, programmerare, säkerhetspersonal men även representanter från systemanvändarna bör finnas med i framtagningsprocessen. Alla de olika personerna har olika utbildningar och erfarenheter och bidrar till datasäkerhetsplanen med olika saker och från olika synvinklar med fokus på datasäkerheten. Pfleeger & Pfleeger (2003) beskriver att andra planer kan användas när en organisation har blivit utsatt för ett hot och man har blivit påverkad av detta på något sätt. Enligt Pfleeger & Pfleeger (2003) specificerar denna plan hur man som organisation ska hantera katastrofsituationer där större delen av datorverksamheten inte kan fungera av olika anledningar eller om datorverksamheten inte kan fungera under en längre tid då brand, mjukvaru-, elektronik-, telefoni- eller nätverkproblem kan vara den utlösande faktorn. Även utvecklingsplaner för att bibehålla datasäkerhet och incidenthanteringsplaner är exempel på andra säkerhetsplaner som utvecklar, bibehåller och utvärderar säkerheten.

Pfleeger & Pfleeger (2003) menar att i en effektiv datasäkerhetsplan ingår det en noggrann riskanalys där man identifierar eventuella problem som systemet eller användarna kan ställas inför

i olika kontexter. Enligt Pfleeger & Pfleeger (2003) pekar riskanalysen på tre olika faktorer – påverkan, problem och kontroll. Påverkan är de negativa effekter som uppstår vid en viss handling och problem uppstår om sannolikheten är hög för att något negativt ska hända vid utförandet av en viss handling. Pfleeger & Pfleeger (2003) menar att om man har kontroll över de handlingar som kan utföras har man eliminerat eller reducerat möjligheterna att problem uppstår. Bace (2000) menar att det kan finnas problem med att särskilja avvikande aktivitet mot användarnas missbruk i de fall då dessa två situationer kan vara av liknande karaktär men ska bli behandlade på olika sätt. De risker som kan uppstå kan reduceras enligt Pfleeger & Pfleeger (2003) med hjälp av tre olika strategier – anta riskens existens, undvika och/eller förflytta riskerna. För att göra en fullständig analys över de risker som organisationen kan råka ut för så framgångsrikt som möjligt menar Bernard (2007) att denna analys måste inkludera personer utanför den egna organisationen men framförallt utanför den egna säkerhetsavdelningen. Vanligtvis tar man hjälp av andra avdelningar för att få olika synvinklar på problemet men detta tillvägagångssätt resulterar i att man endast får en liten del av riskbilden klar för sig. Genom att identifiera samtliga tillgångar i form av mjuk/hårdvara, data, användare och dokumentation menar Pfleeger & Pfleeger (2003) att man har en grund till att se de områden där organisationen är sårbar på något sätt med hjälp av de grundläggande säkerhetsbegreppen – sekretess, integritet och tillgänglighet. Nästa steg i processen som Pfleeger & Pfleeger (2003) beskriver är att analysera sannolikhen att problemet uppstår och beräkna den förväntade ekonomiska förlusten som kan uppstå. Sista steget är att hitta och utvärdera lösningar som motverkar de problem man funnit som kan uppstå och applicera minst en försvarsteknik på varje funnen sårbarhet.

Efter det att risken blivit identifierad finns det enligt Jones (2007) fyra olika sätt att motarbeta denna risk beroende på riskens påverkan på organisationen och frekvensen för hotet. Ett sällan återkommande hot som inte påverkar organisationen mer än vad som är acceptabelt är ett hot som bör accepteras av organisationen. Jones (2007) menar att antalet hot och nivån på de hot som organisationen accepterar visar organisationens utsatthet men även deras medvetenhet. Skulle hotet återkomma oftare men samtidigt ha samma påverkan på organisationen som föregående exempel så är en förflyttning av hotet att rekommendera. Skulle däremot påverkan på organisationen bli hög anser Jones (2007) att andra åtgärder måste tas. Vid hög påverkan på organisationen men sällan återkommande hot rekommenderas att man reducerar riskerna genom att införa tekniska lösningar som stoppar alternativt synliggör hoten som organisationen ställs inför. Skulle införandet eller förändring av mjukvara eller hårdvara ge oönskade konsekvenser på datasäkerheten i form av hög frekvens av hot samtidigt som påverkan på organisationen bli stor anser Jones (2007) att man bör undvika hotet genom att begränsa eller undvika att införandet eller förändringen.

3.3.5. Medvetenhet

För att undvika att man antar att organisationens datasystem är säkert föreslår Panko (2004) att man anlitar ett externt företag som övervakar och försöker hitta svagheter i organisationens datasäkerhetslösning. Detta ger enligt Panko (2004) en realistisk bild över hur säkerheten fungerar. Panko (2004) menar att det kan vara svårt att hitta pålitliga säkerhetstestare då känslig information om organisationens säkerhet kan hamna i orätta händer, men rekommenderas ändå då resultatet blir bättre i jämförelse med program som finns som automatiskt kontrollerar säkerheten på en relativt grundläggande nivå. Knapp, Marshall, Rainer Jr, & Morrow (2006) menar att många av dagens företag är beroende av IT och enligt deras undersökning bekräftas det att stödet och initiativet från organisationens ledning måste finnas om ett säkerhetsmedvetande ska existera. Om ledningen inte anser att säkerhet är viktigt är risken stor att även resten av organisationen anser detta. Polaniecki (2006) menar att företagsledningen ska ha ett förtroende

för de anställda som hanterar säkerhetsfrågorna i företaget. Genom att ställa en del frågor till företagsledningen så kan de säkerhetsansvariga uppmärksamma vissa risker för företagsledningen. Polaniecki (2006) beskriver frågor som belyser bland annat en utvärdering av vilken riskpotential vissa delar av systemen har, hur är den fysiska säkerheten, vad händer vid en katastrof och hur skyddad är vår data.

Enligt Bace (2000) finns det flera olika sätt att övervaka ett system och varje sätt samlar på olika typer av data från olika situationer och på olika nivåer. Oavsett vilket sätt man övervakar på samlar man in information och låter denna information analyseras för att hitta symptom för onormalt beteende hos användare, eller andra aktörer, som kan påverka den skyddade informationen. Denna analys kan enligt Bace (2000) göras i två olika syften som inte alltid görs tillsammans då man väljer att endast använda sig av ett syfte, antingen hitta missbruk eller onormal användning och det är i vissa fall svårt att särskilja dessa två. Bace (2000) menar att stora fördelar kan uppnås om man använder sig av båda typerna då man letar efter onormal användning för att hitta nya eller okända attacker. Bace (2000) menar att ovanpå denna teknik används missbruksdetektion som säkerställer att onormalt beteende inte blir normalt beteende eftersom en viss typ av attack kan verka normal efter en period. Denna säkerställning körs enligt Bace (2000) mot organisationens uppsatta säkerhetspolicys som finns definierade.

3.4. Policy

En säkerhetspolicy ska kunna beskriva syftet med de säkerhetsfunktioner som finns men också kunna besvara tre frågor som ställs om vilka som har tillgång till *vilka resurser* och på *vilket sätt* och med *vilken utrustning* eller metoder det ska göras (Pfleeger & Pfleeger, 2003). En säkerhetspolicy ska enligt Pastore & Dulaney (2006) vara en vägledning för personerna i en organisation för hur de ska bete sig för att bibehålla en god datasäkerhet genom att ge en generell bild över kraven som ställs. Anledningen till att den skrivs så pass generell är enligt Pfleeger & Pfleeger (2003) för att slippa skriva om den så ofta eftersom små förändringar ständigt sker. Fyra syften med en dokumenterad datasäkerhetspolicy är att:

- känna igen känslig information
- klargöra ansvarsområde för användarna
- skapa en insikt hos befintliga användare
- guida nya användare

Pfleeger & Pfleeger (2003) menar att en god datasäkerhetspolicy ska vara generell så att den blir hållbar i tiden, även efter små uppdateringar, men ändå kunna täcka de möjliga situationer som kan uppkomma. Denna typ av policy måste vara realistisk för att den ska kunna följas bland annat ur användnings- och ekonomiska perspektiv. Pfleeger & Pfleeger (2003) menar även att en policy ska vara skriven på ett sätt som möjliggör att läsarna ska kunna läsa och förstå innehållet för att policyn ska implementeras och användas fullt ut. En datasäkerhetspolicy ska specificera organisationens säkerhetsmål och vem som har ansvaret för dessa och organisationens inställning till datasäkerhet.

3.4.1. Säkerhetspolicy

Pfleeger & Pfleeger (2003) och Mitrović (2005) beskriver en säkerhetspolicy som en redogörelse för hur ett system ska erhålla den datasäkerhet som organisationen önskar. Enligt Mitrović (2005) måste man veta vilken typ av säkerhet man behöver och denna ska uppdateras efter hand beroende på organisationens hotbild som anpassas efter de hot, svagheter och sårbarheter som organisationen upplever. Vidare menar man att en säkerhetspolicy även ska innehålla olika motåtgärder i form av fysiska, logiska och administrativa åtgärder. Beroende på antalet motåtgärder och dess styrka varierar kostnaden för den aktuella datasäkerheten. Pfleeger & Pfleeger (2003) och Mitrović (2005) menar även att olika säkerhetsnivåer är viktiga att finna och tilldela olika tjänster inom organisationen då de olika nivåerna beskriver hur säkerheten är för organisationen samt hur stor skada som uppstår vid problem. Åtgärder som måste implementeras oavsett skadenivå eller teknikområde är spårbarhet, åtkomstkontroll men även identifiering och autensiering. Vidare menar de att när detta är gjort kan man utföra en hotbildsanalys inom varje teknikområde och utvärdera styrkor, svagheter, konsekvenser, motåtgärder och kostnader.

Enligt Panko (2004) är en av de viktigaste delarna inom datasäkerhetsområdet kontrollen över vilka som har tillgång till en viss data och vad denna specifika användare kan göra med denna data. Panko (2004) menar att detta är en policydriven skyddsmekanism och hindrar hackers och andra ovälkomna användare till åtkomst eller modifikation av en viss data. Att bestämma vilken data som ska skyddas, på vilket sätt den ska skyddas och identifiera de olika rollerna som ska ha olika behörigheter till den skyddade datan är en del av säkerhetsarbetet. Denna behörighetskontroll kan enligt Panko (2004) ske på olika sätt som är lämpliga för att kunna avgränsa antalet användare som har åtkomst till de skyddade delarna. De olika sätten man väljer för att skydda viss data och alla konfigurationer ska dokumenteras och sammanställas i en del av organisationens säkerhetspolicy.

Pfleeger & Pfleeger (2003) beskriver grundprincipen med bland annat den datasäkerhetspolicy som militären använder för att skydda information och endast låta en viss målgrupp få ta del av en viss typ av information. Pfleeger & Pfleeger (2003) beskriver att det inom militären finns olika klassificeringsgrader på information och dessa kopplas mot militärens hierarkiska system och därmed säkerställs vilka personer som kan få ta del av en viss information. Även grupper med blandade behörighetsgrader kan sättas samman och som grupp kan man få en viss befogenhet att läsa viss information. En annan typ av säkerhetspolicy är en kommersiell säkerhetspolicy där nyckelorden för behörighet är offentligt, internt och privat där den offentliga informationen, enligt Pastore & Dulaney (2006) endast uppgår till 20 procent och resterande 80 procent är skyddad på något sätt. Dessa nyckelord varierar från organisation till organisation medan förhållningssättet mot känslig och mindre känslig information finns i alla situationer. Skillnaden som Pfleeger & Pfleeger (2003) framför är att om man i den kommersiella policyvärlden har tillträde till den interna informationen har man därmed tillträde till all information som finns i det interna informationsnätverket, medan det militära har olika grader av tillit som ger användaren tillträde till en viss typ av information i den interna informationen. Ovanstående datasäkerhetspolicys har fokuserat på sekretessdelen som är en byggsten i säkerhetskonceptet. Dock återstår det två anda viktiga delar för att få en komplett och god säkerhetslösning, integritet och tillgänglighet, och även för dessa två finns det olika policys som fokuserar på dessa termer. Pfleeger & Pfleeger (2003) beskriver en säkerhetspolicy vid namn Clark-Wilson Commercial Security Policy som fokuserar på integritet hos information och på så sätt skapar tillit i transaktioner som sker i ett visst moment. Genom att göra saker i rätt ordning skapar man ett gott flöde i arbetsprocessen med rätt information. Andra policys som Pfleeger & Pfleeger (2003) beskriver fokuserar på att rätt personer ska göra rätt saker och att användare ska använda ett

begränsat antal funktioner för att kunna utföra de arbetsuppgifter som man är ålagd att göra och därmed inte använda andra funktioner även om man har tillgång till andra funktioner.

3.4.2. Lösenordspolicy

Panko (2004) och Stallings (2003) menar att användning av lösenord är första nivån i en god datasäkerhet och att hantera denna del otillräckligt är samma sak som att inte använda lösenord överhuvudtaget. Att använda lösenord för att skydda sin data på ett effektivt sätt anser Panko (2004) och Stallings (2003) att det behövs en lösenordspolicy som grund där lösenordens karaktär och användningsområden ska vara specificerade. Vidare anser de att en god lösenordspolicy bör innehålla riktlinjer hur ett bra och därmed godkänt lösenord ska vara uppbyggt med antal-, tillåtna-, förbjudna- och obligatoriska tecken. Denna sortens policy ska även innehålla lösenordets förnyelseintervall, hur man hanterar avaktiverade konton, intervall och metod för test av lösenord och förlorade lösenord men även hur man hanterar denna viktiga information i form av användaruppgifter och lösenord. Genom att ha en stark och tydlig policy angående lösenord och dess hantering menar Panko (2004) och Stallings (2003) att en trygg tillvaro skapas med minimala lösenordsrisker.

3.5. Säkerhetsmodeller

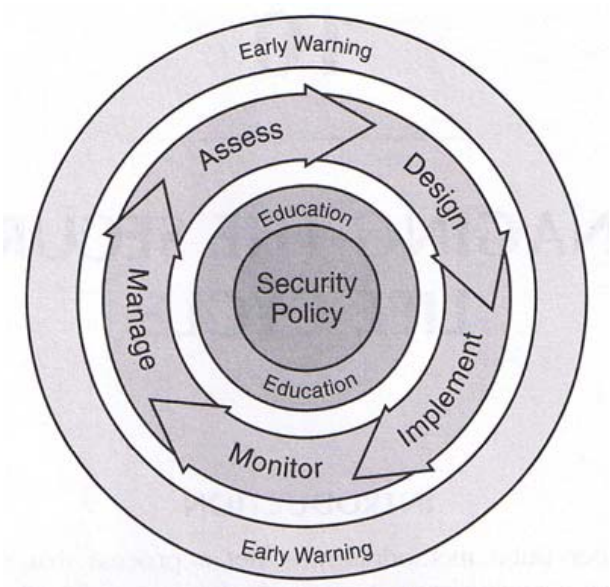
Pfleeger & Pfleeger (2003) menar att en säkerhetsmodell är som precis som andra modeller, den hjälper till att utveckla, testa, underhålla och utvärdera lösningar för en viss organisation. Dessa säkerhetslösningar kan vara i form av policys som upprätthåller en säkerhetsvision som organisationen har. Pfleeger & Pfleeger (2003) beskriver att det finns olika modeller som är inriktade mot säkerhet på olika sätt. Vidare menar Pfleeger & Pfleeger (2003) att det är nödvändigt att skapa och analysera olika modeller för att kunna skapa bra säkerhetspolicys och säkra system som hanterar känslig data. Tittel, Hudson & Stewart (1999) beskriver en säkerhetsmodell där användaren står i relation till den information som organisationen önskar skydda. En användares åtkomst till organisationens information kan regleras med två olika grundtyper av kontosäkerhet - delningsnivå och användarnivå. Tittel, Hudson & Stewart (1999) anser att delningsnivån bestämmer åtkomsten till en viss resurs och ägaren till denna resurs bestämmer lösenord och endast de som känner till lösenordet kan ta del av resursen. Den andra typen av säkerhetsnivå är användarnivå och då tilldelas en användare en viss behörighet mot nätverk och resurser.

3.5.1. Skiktad säkerhetsfilosofi

McCumber (2005) menar att skiktad säkerhet är en grundläggande filosofi som är en nödvändig komponent i ett större IT-system för att bibehålla säkerhet. Genom att ringa in den information som ska skyddas av olika typer av användare får man en stor cirkel med en mindre cirkel inuti, som i sin tur har en ännu mindre inuti sig. Den innersta cirkeln omsluter den information som är mest känslig och skyddas som hårdast och den information som finns utanför den yttersta är information som samtliga har åtkomst till. McCumber (2005) menar att varje ring är till för att reducera specifika sårbarheter och den yttersta ringen har inte samma typ eller styrka på säkerheten som det finns ju närmare mitten man kommer.

3.5.2. Säkerhetslivscykel

McCumber (2005) beskriver en säkerhetslivscykel (se Figur 4) som är inspirerad av *Symantec Corporation's Lifecycle Security ™ Model* och ska vara till hjälp för att föreställa, skapa tillämpa och utvärdera strategier för god säkerhetshantering.



Figur 4: Säkerhetslivscykel (McCumber, 2005, s. 166)

McCumber (2005) beskriver att den del av livscykeln som är iterativ är den del där analys, design, implementation, övervakning och hantering är belägna då hotbilden mot organisationen och säkerhetssituationen inte är konstant. McCumber (2005) menar att en god säkerhetspolicy tillsammans med utbildning av användarna och regelbunden iteration enligt modellen ska skapa en tidig varning för den säkerhetsansvariga personalen och på så sätt kunna anpassa säkerhetslösningarna efter det hot som uppstått. Utbildningen är inte en utbildning endast för personer med det yttersta säkerhetsansvaret utan det ska vara utbildning för samtliga användare som hanterar den data som säkerhetsreglementet är skapade för.

4. Empirisk undersökning

4.1. Intervju med MOROTSmedia

MOROTSmedia är del av en liten koncern där MOROTSmedia, Distributed Medical och Perspektiv Bredband ingår. MOROTSmedia är ett eget konsultbolag som jobbar med system- och programvaruutveckling och har 5 anställda och tillsammans har koncernen 36 anställda varav 25 personer på Perspektiv Bredband. Filip Strandqvist arbetar som konsult och VD på företaget och har därmed även interna uppdrag som berör andra delar av koncernen med bland annat affärsutveckling och administrativa uppdrag.

Intervjun med MOROTSmedia ägde rum i deras lokaler i Lund, i deras konferensrum som också fungerar som ett demorum för Distributed Medical. Den information som MOROTSmedia avser att skydda är känslig information, antingen för de själva eller för deras kunder. Företaget har tillgång till mängder av information hos andra företag med hjälp av olika VPN-uppkopplingar och i detta fall handlar det mycket om vilka personer som ska ha tillgång till vilken typ av information. Därför anser Filip Strandqvist att man har goda arbetsstyrda rutiner, hanterar lösenord, in- och utloggningar på ett bra sätt. I en konsultverksamhet är det viktigt att kunna anpassa sig och leva upp till kundernas säkerhetspolicy och säkerhetsvärderingar. Filip Strandqvist anser att MOROTSmedia har en hög datasäkerhetsmedvetenhet då deras verksamhet är väldigt tekniskt orienterad men menar även att datasäkerhet kan uppfattas olika beroende på vilka man frågar. För MOROTSmedia är datasäkerhet viktigt och de slår ett slag för ett gott helhetsbegrepp. ”Vi har ganska hög datasäkerhetsmedvetenhet inom vår verksamhet för att vi är så teknikorienterade.” (Filip Strandqvist, personlig kommunikation, 15 maj, 2007)

Att bara förlita sig på lösenord och andra liknande säkerhetslösningar är inte att rekommendera då den fysiska säkerheten är lika viktig. MOROTSmedia har bland annat pansarglas i sin lokal och har goda rutiner att stänga och låsa dörrar efter sig, även om det skulle bara bekvämt att låta dem stå öppna. Den information som MOROTSmedia lagrar är oftast oväsentlig och ointressant för andra företag men väldigt viktig för MOROTSmedia. Den reella risken som finns för företaget är att någon vill ha själva utrustningen i form av datorer, tv-apparater m.m. istället för innehållet på dessa. Det värsta som skulle kunna hända MOROTSmedia skulle vara om någon som har glädje av den information som de lagrar och gör ett inbrott, antingen ett nätmässigt eller fysiskt, och tar del av denna information, men det har Filip Strandqvist svårt att tänka sig att det ska hända. Det skulle i så fall vara ett företag som konkurrerar ”head on” med MOROTSmedia och som hade samma kunder som skulle kunna utgöra denna typ av hot, men något sådant företag finns inte enligt Filip Strandqvist. Ännu värre skulle det vara om den stulna informationen inte var MOROTSmedias då det skulle bli svårt att förklara att informationen försvunnit eller kommit i någon annans händer för att de har bristande datasäkerhet. Då mycket av den information som MOROTSmedia har är någon annans från början så är denna extra känslig att bli av med då denna information är extremt viktig för kunden. Dock blir MOROTSmedias information snabbt värdelös då de arbetar med färsk information. Intrångsservers registrerar allmänna hot som alltid förekommer såsom DDoS-attacker och diverse robotar men detta sker på en normalt låg nivå och ses inte som ett reellt hot för verksamheten. Då samtliga anställda på MOROTSmedia, enligt Filip Strandqvist, är IT-nördar så har begreppet sunt förnuft ett högre datasäkerhetsvärde jämfört men andra företag inom andra områden. ”Jag tror den största reella hotbilden, inte är industriella

spioner eller någon som faktiskt vill anstränga sig för att stjäla information. […] Jag tror det största reella hotet vi har här är just att de bryter sig in" (Filip Strandqvist, personlig kommunikation, 15 maj, 2007)

Det finns policys i verksamheten och ett kapitel i en personalhandbok handlar om IT-säkerhet i varje bolag i koncernen och i den finns riktlinjer hur man upprätthåller god datasäkerhet. Grundprincipen i denna handbok är att man är förpliktigad att skydda den data man har tillgång till genom sin anställning på ett förnuftigt sätt. De nyanställda får även en mindre föreläsning där datasäkerhet är en av punkterna. Skulle det någon gång hända något i stil med att en bärbar dator försvinner för att man brutit mot någon av de tumregler som finns brukar tumreglerna upprepas så att man håller de färska. Det är lätt att sådana här händelser händer någon gång per år vid exempelvis inbrott i en bil. De arbetar även i liten grad med att utveckla policys på begäran åt andra företag och resultatet av detta kan vara en handbok som man senare ger utbildning i där man berättar vad som är viktigt att tänka på samt vilka konsekvenser som kan uppstå vid felaktigt beteende. Lösenordshanteringen på MOROTSmedia består av krypterade och starka lösenord som roteras med jämna mellanrum, och detta är en av de punkter som tas upp i den tidigare omnämnda handboken. Andra viktiga saker är att man inte får lämna datorn utan att logga ut eller stänga av skärmen och man får heller inte kopiera information till USB-minnen för att kunna ta hem dessa för att det är smidigt. Detta är enkla tumregler som MOROTSmedia har för sina anställda för att en säkrare miljö ska råda.

När MOROTSmedia utvecklar nya system från grunden arbetar de med att säkerställa en god säkerhetsmiljö bland annat genom att införa lösenordskontroller och andra adekvata säkerhetslösningar och detta kan kopplas till kundens användardatabas och på så sätt följa deras standarder. Då MOROTSmedia implementerar och bygger system från grunden är en viktig del att försäkra sig om att det nya systemet är säkert men även om systemet kommunicerar med andra system ska även denna kommunikation vara säker. Ett annat sätt kan vara att arbeta med kunder och deras nuvarande säkerhetslösningar för att sedan kunna förbättra dessa genom utbildning eller nya rutiner för att höja säkerhetsmedvetandet. Det kan i detta fall handla om att skriva en handbok och/eller hålla några workshops med personalen.

Någon skillnad mellan ledning och anställda anser inte Filip Strandqvist att det finns hos MOROTSmedia av den anledningen att de är en platt organisation då alla anställda verkar på samma nivå. I andra organisationer som de kommit i kontakt med är det alltid någon från ledningen som har kommit med initiativet att göra en förändring och oftast är det någon händelse i form av att en dator blir stulen eller något liknande som triggar i gång denna process. Filip Strandberg tror inte att man kan säga att det finns något generellt att ledningen är inkompetenta och de anställda har god säkerhetskännedom eller tvärtom. Han kan inte svara för om det finns en generell skillnad mellan ledning och de anställda i andra företag.

Spam är enligt Filip Strandqvist ett hanterbart problemområde med hjälp av tekniska hjälpmedel. Etiskt inkorrekta mail finns det ingen lösning mot men i de fall man kommit i kontakt med dessa på andra företag har man löst detta genom att undersöka var mailet kom ifrån, sedan får personalavdelningen ta tag i detta problem med en muntlig kommunikation. Andra kontrollerande situationer som Filip Strandqvist varit med om är i bankvärlden där man är ganska strikt och kontrollerar vilka hemsidor som de anställda besöker på arbetstid och vidtar åtgärder därefter. Filip Strandqvist tror att det säkerligen finns det svenska företag som är väldigt kontrollerande men MOROTSmedia är inte ett av de företagen. Då det enligt lag är förbjudet att läsa andras mail och avlyssna de anställda så tror Filip Strandqvist att den svenska företagskulturen är ganska okontrollerad i det avseendet. Svenska företag kontrollerar exempelvis de anställda och deras arbetsrutiner då de märker att något inte står rätt till för att ställa saker och

ting till rätta. ”Generellt kan man säga att amerikanska företag tenderar att vara väldigt mycket striktare i jämförelse med svenska företag. Banker tenderar också att vara väldigt strikta.” (Filip Strandqvist, personlig kommunikation, 15 maj, 2007)

Karaktäristiska drag hos MOROTSmedia:

- litet företag (5 anställda)
- huvudsakliga uppgifter är systemutveckling
- utvecklar även policys och handlingsplaner på begäran
- tekniskt kunniga anställda
- deras reella hot är mot den fysiska säkerheten
- anser sig ha god datasäkerhetsmedvetenhet
- har tillgång till mycket information hos deras kunder
- anser sig inte ha någon direkt konkurrent
- har utformade policys
    - datasäkerhetspolicy
    - lösenordshantering
    - informationshantering
    - hur man hanterar utrustning för att minimera stöld
- utbildar för att upprätthålla god datasäkerhet
- ingen skillnad mellan ledning och anställdas syn på datasäkerhet (platt organisation)
- detaljerad och avslappnad intervju

4.2. Intervju med Atea i Sverige

Atea är en del av en nordisk koncern med 20-talet kontor över hela Sverige. I Sverige består Atea av ca 1000 anställda som tillsammans hjälper företag och organisationer genom att leverera och sälja produkter och tjänster som förenklar hantering, drift och utveckling av IT-infrastruktur såsom behörighetssystem, katalogtjänster, digitala certifikat och många fler. Företaget finns i samtliga länder i norden men går under olika företagsnamn – Ementor i Norge, Top Nordic i Danmark och Atea i både Finland och Sverige.

Intervjun med Atea i Sverige ägde rum på ett av deras kontor i Sverige med en erfaren konsult inom IT-säkerhet och med flertalet certifikat i meritlistan. Konsulten hos Atea i Sverige arbetar uteslutande med IT-infrastruktur där kontakten mot kunden är viktig då utbildning, rutiner och processer är en del av arbetet. Konsulten generella syn på datasäkerhet är fokuserad kring den fysiska och den logiska datasäkerheten. Konsulten svarar på frågor och ställer dem i relation till deras arbetssätt mot de kunder de har då det egna säkerhetsarbetet sätts i skymundan just på grund av att de fokuserar mer på deras kunder än på sig själva. ”Skomakarens barn går ju alltid med de sämsta skorna” (konsult på Atea i Sverige, personlig kommunikation, 10 maj, 2007). Enligt konsulten själv så är deras egna skydd tillräckligt då de själva har information som exempelvis kundregister och absolut inte får komma i konkurrenternas händer men menar även att deras datasäkerhet skulle kunna vara bättre. Anledningen till detta tror sig vara att de satsar mer på sina kunder än på sig själva och deras datasäkerhet. De anställda på Atea i Sverige är tekniskt lagda personer och detta tror konsulten kan vara en anledning till den lågt hållna säkerhetsfilosofin då de anställda vet mycket mer om säkerhet än många andra och tillämpar därmed mer sunt förnuft och är mer försiktiga, men konsulten framför att det finns riktlinjer för hur man får bete sig.

Konsulten arbetar direkt med kunderna och samlar på sig erfarenheter samtidigt som han delar med sig av den kunskap som han och företaget besitter och detta anser konsulten vara en av fördelarna med att vara konsult. Detta gör att konsulten har en bred uppfattning av säkerhetsläget då han ser många olika hotbilder, säkerhetslösningar, händelser och incidenter men anser att han inte klarat arbetet utan kundens insyn i sin egen verksamhet då de ser olika händelser och incidenter på ett annat sätt. I många fall har inte kunderna någon säkerhetsfilosofi applicerad på verksamheten och då försöker Atea i Sverige övertyga eller påvisa kunden att denna behöver ha en högre nivå av säkerhetstänkande. I de fall då kunden redan har en väldefinierad säkerhetsfilosofi tar konsulten erfarenhet av kundens riktlinjer. Någon skillnad mellan de anställda och ledningens säkerhetsuppfattning på Atea i Sverige har inte konsulten uppfattat utan anser att de båda parterna har en gemensam uppfattning. Däremot finns det en stor skillnad mellan kundens it-personal och deras ledning, där ledningen inte är medveten över de risker som finns.

Själva arbetet med att utveckla en säkerhetslösning för en kund börjar med en riskanalys för att få en bild över de mest kritiska tillgångarna och sedan utvärdera vilka hot dessa står inför. Kunden får sedan prioritera sina säkerhetsinvesteringar och satsa sina säkerhetsinvesteringar på ett annorlunda sätt än tidigare om kunden har prioriterat och investerat på ett annat sätt. Det rekommenderas även att utbildning och regelbundna utvärderingar kring säkerhetsfrågorna görs men även att företagsledningen har en öppen och frekvent dialog kring säkerhetsfrågor. I prioriteringsfrågorna håller konsulten en låg profil då konsulten anser att kunden har en betydligt bättre kunskap och vet bäst hur både sina egna system fungerar och den dels den egna verksamheten, om bara en eftertanke finns. Konsulten framför att det finns en risk att kunden prioriterar felaktigt men menar att om kunden funderar på de viktigaste tillgångarna de har kan besluten bli mer korrekta. Konsulten menar även att man som konsult aldrig kan förutse alla händelser som kan uppstå mot en verksamhet men med en väl genomtänkt plan finns förhoppningarna att skapa en god lösning och därmed vara mer förberedd. ”I och med att säkerheten har blivit så mycket viktigare så krävs det mer och mer resurser för att klara av bra informationssäkerhet” (konsult på Atea i Sverige, personlig kommunikation, 10 maj, 2007). De rekommendationer som Atea i Sverige ger kunden angående denna typ av analys är att den bör återkomma en gång om året för att göra en uppföljning samt göra små förändringar på de punkter företaget har förändrats.

Policys finns i en begränsad mängd då man på Atea i Sverige har policys för etiska regler för internet- och mailanvändning, krav på att de lösenord som finns ska vara starka lösenord samt har även en it-säkerhetspolicy. Andra regler som kan specificeras i policys som konsulten stött på kan vara vilka internet sidor man som anställd får besöka. Konsulten menar att policys som berör diskriminering i olika former behövs i varje verksamhet. Nästa steg är att kontrollera om dessa policys efterföljs och detta hamnar enligt konsulten ofta i andrahand då det finns viktigare saker att göra. Däremot hjälper de sina kunder med att utforma policys i samråd med kunden och ett flertal exempelmallar som anpassas efter företagets behov. Det är enkelt att kontrollera om det policys som finns efterföljs men det är en stor etikfråga. Den stora frågan är hur mycket tekniken ska få kontrollera utan att de anställdas integritet störs. Konsulten anser att det kan vara viktigare att ha en utbildning, som Atea i Sverige själva även använder sig av, i de olika policys som finns istället för att kontrollera de anställda. Skulle det uppmärksammas att det är någon som bryter mot reglerna så skulle detta leda till åtgärder.

Då konsulten inte har varit med när analysen av säkerheten på Atea i Sverige gjordes antogs det att den värsta händelsen, ut ett datasäkerhetsperspektiv, skulle vara att kundlistan fanns tillgänglig för konkurrenterna. Denna händelse kan vara förödande för Atea i Sverige, då förtroendet minskar, men även förödande för kunden som anlitat Atea i Sverige. En annan känslig punkt som

Atea i Sverige har, är att i utredningsstadiet skapas och lagras viktig och känslig information om en kund och denna information får inte heller finnas tillgänglig för utomstående.

För att säkerställa den mänskliga riskfaktorn använder de sig av utbildning där IT-säkerhetspolicys och etiska perspektiv gås igenom så att ökad försiktighet råder med de uppgifter som berör kunder men även för att kunna vara rättvis. Atea i Sverige arbetar även med att säkerställa att den information som de anställda har inte kan spridas så snabbt när en person avskedas. Reglerna säger att de anställda inte får ha två arbeten parallellt och under uppsägningstiden läcka något till sin nya arbetsgivare. Den anställde får heller inte byta till ett konkurrerade företag efter en viss tid efter uppsägningen. Konsulten menar att det funnits sådana här regler tidigare men har ingen större kunskap om hur reglerna är utformade i dagsläget.

Karaktäristiska drag hos Atea i Sverige:

- stort företag (ca 1000 anställda i Sverige)
- huvudsakliga uppgifter är konsultation och implementering av IT-infrastrukturlösningar
- utvecklar även policys tillsammans med kund
- konsulterna är teknikkunniga
- kundlistan är den mest skyddade informationen
- har konkurrenter
- anser sig ha mycket god datasäkerhetsmedvetenhet
    - deras kunders datasäkerhet prioriteras högre än deras egna
- har utformade policys
    - etiska regler för Internet- och mailanvändning
    - lösenordskrav
    - it-säkerhetspolicy
- utbildar för att upprätthålla god datasäkerhet
- anser att ledning och anställda har en gemensam syn på datasäkerhet
- stel intervju med tillfredställande intervjusvar

5. Analys

5.1. Skillnader och likheter mellan företagen

Det är stor skillnad i storlek på de båda företagen då MOROTSmedia har 5 anställda och Atea har ca 1000 i Sverige. De båda företagen arbetar nära kunder och detta med utvecklings- och konsultverksamhet. Atea i Sverige utvecklar IT-infrastrukturlösningar medan MOROTSmedias fokus ligger närmare systemutveckling. Att det skulle skilja i storlek på företagen samt att de skulle ha ett gemensamt verksamhetsområde var ett krav från vår sida, då vi ville undersöka om storleken hade någon betydelse i datasäkerhet och medvetenheten kring denna. De båda respondenterna har erfarenhet inom konsultation då det är deras huvudsakliga syssla, men konsulten på MOROTSmedia arbetar närmre den egna organisationens kärna då han även har en titel som VD. Då båda arbetar som konsulter och ofta berör ämnet datasäkerhet i sin yrkesroll så anser de sig vara väl insatta i datasäkerhet och därmed medvetna om de risker som finns i omgivningen men även konsekvenser som kan uppstå. Trots storleksskillnaden så anser vi att båda företagen har ett tillräckligt likt verksamhetsområde för att ingå i studien.

Båda företagen anser att de har viktig information som de skyddar mot utomstående. Bernard (2007) menar att säkerhet är viktigt oavsett lagringsmedia. Information i pappersform är av lika stor vikt som den mer uppmärksammade informationen som är lagrad i elektronisk form. MOROTSmedia har åtkomst till flertalet informationskällor där de kan hämta verksamhetsnära information hos kunden som behövs för att utföra ett uppdrag. Denna information skyddas på det sätt som Panko (2004) föreslår då man har kontroll över vilka personer som har tillgång till en viss data. En del av den information de lagrar blir snabbt inaktuell och anses vara värdelös för en person eller annat företag då MOROTSmedia är det enda företaget som utför denna typ av uppdrag. Det är alltid känsligt när information som inte är ens eget försvinner, på grund av slarv eller bristande säkerhet, vilket gör att företaget mister förtroende och kunden blottas och kan på det sättet skadas. Liknande situation finns hos Atea i Sverige där man i utredningsstadiet har samlat ihop en viss typ av information som kan vara skadlig på samma sätt som i fallet med MOROTSmedia där kund och det egna företaget far illa när informationen kommer i orätta händer. I denna typ av situation menar Pfleeger & Pfleeger (2003) att det är nödvändigt med säkerhetspolicys och säkra system för att kunna hantera känslig data på ett säkert sätt.

Synen på mänsklig, logisk och fysisk säkerhet skiljer sig inte mycket mellan de två företagen. Logisk säkerhet är något som för företagen är givet på grund av den viktiga information som företagen har men också för att de innehar den tekniska kunskapen för att förstå att det är viktigt. MOROTSmedia påpekade att personer med hög teknisk kunskap oftast har högre medvetande gällande datasäkerhet, särskilt inom den logiska säkerheten. Båda företagen nämner och förklarar också vikten av mänsklig säkerhet i form av utbildning, policys och sunt förnuft. Ett företag med endast fem väldigt teknikkunniga personer, som MOROTSmedia, används sunt förnuft på grund av att alla de anställda redan innehar en stor kunskap om datasäkerhet. Hos ett större företag med ca 1000 anställda som Atea i Sverige har, bör sunt förnuft blandas med tydliga riktlinjer och regler på grund av att vissa anställda inte innehar kunskapen om datasäkerhet. MOROTSmedia lägger större fokus på fysisk säkerhet under intervjun än vad Atea i Sverige gör och menar att ett fysiskt hot är det mest reella hotet för dem som företag. Pfleeger & Pfleeger (2003) menar att den fysiska säkerheten ofta kan uppstå genom sunt förnuft.

Fysisk säkerhet anser vi är precis som Pfleeger & Pfleeger (2003) en given aspekt av datasäkerhet och Mitrović (2005) anser att det inte lönar sig att ha bra logiska skydd om det inte finns god fysisk säkerhet. Bernard (2007) påpekar att all information som är av vikt behöver skyddas på något vis till exempel att information i pappersform ska skyddas fysiskt. Fysiskt skydd är något man kan räkna in i det sunda förnuftet och hos företag är det en självklarhet att man ska ha bra lås och larm för att minska riskerna för till exempel inbrott. Att MOROTSmedia lade större fokus på fysisk säkerhet under intervjun behöver därmed inte betyda att Atea i Sverige har en sämre fysisk säkerhet.

Synen på datasäkerhet skiljer sig endast lite mellan företagen men detta anser vi är på grund av att man måste ha ett visst synsätt gällande datasäkerhet för att konkurrera på konsultmarknaden. McCumber (2005) menar att datasäkerhet är kontextberoende och vi anser att datasäkerheten skiljer sig mellan företagen på grund av dess kontextolikheter. Företagens syn på datasäkerhet, vad som är av vikt och så vidare, skiljer sig dock inte lika markant.

5.2. Hotbild

De hot som de båda företagen står inför är på vissa punkter lika då de båda har information tillhörande eller om andra företag som absolut inte får komma i fel händer. Atea i Sverige har kundregister och utvärderingsmaterial som ska skyddas då dessa är känsliga både för företaget och för deras kunder. Någon närmare information om hur, var eller varför dessa skyddas framgår inte ur intervjun och den konsult vi intervjuade hade inte heller medverkat eller tagit del av den säkerhetsanalys som man gjort på företaget och kunde därför inte svara med 100 procents säkerhet vad som skulle vara det värsta som kunde hända företaget ur ett datasäkerhetsperspektiv. Konsulten medger även att deras skydd är tillräckligt men också att deras skydd inte är lika bra som det skulle kunna vara då de satsar väldigt mycket på sina kunder och de själva hamnar i skymundan. Även MOROTSmedia har information som de skyddar mot utomstående men då de har en annorlunda hotbild jämfört med den bild som Atea i Sverige har gett oss skyddar de även sin information annorlunda. MOROTSmedia har satsat en del på den fysiska säkerheten i form av pansarglas, strikta rutiner om att låsa dörrar efter sig, logga ut datorn när man lämnar den och stänga av datorskärmen när man lämnar arbetsplatsen för dagen. Deras reella hot som de framför till oss är just den fysiska hotbilden där man är rädd att datorer och annan utrustning blir stulen och därigenom även den information som finns lagrad på denna. Periodvis är detta en stor risk för företaget och detta säkerhetselement har man tagit fasta på och anpassat och fastställt en del regler för att minska riskerna för stöld. Skulle ett intrång ske skulle anledningen för detta vara att stjäla den tekniska utrustning som de äger istället för att vara intresserade av den data som finns, då denna varken är användbar eller intressant för utomstående. Den intrångsserver som MOROTSmedia använder sig av registrerar ständigt försök av intrång och diverse attacker men alla är så pass ofarliga att ingen ytterligare åtgärd behövs.

Vi anser att det är naturligt för ett företag att skydda den data som de anser vara viktig, precis som både Atea i Sverige och MOROTSmedia gör. Pfleeger och Pfleeger (2003) anser att detta skydd planeras och utvecklas med hjälp av en datasäkerhetsplan där man identifierar eventuella problem som systemet eller användarna kan ställas inför i olika kontexter. Att anpassa det skydd man väljer efter den typ av data och i vilken grad av utsatthet denna befinner sig i är lika naturligt (Mitrović , 2005; Panko, 2004). Olika typer av data i olika typer av organisationer skyddas på olika sätt just därför att det finns olika värderingar om vilken data som anses vara viktig men även andra faktorer spelar in (Panko, 2004). MOROTSmedia skyddar sin verksamhet även på det fysiska planet just för att sannolikheten för inbrott periodvis är hög i det område där deras lokaler

finns. Andra termer kring datasäkerhet enligt Panko (2004) och Mitrović (2005) är logisk och mänsklig säkerhet. De båda företagen har en väl utvecklad säkerhet inom dessa områden och detta anser vi beror på den höga tekniska kunskapen som finns i företagen.

5.3. Upprätthållande av datasäkerhet

De båda respondenterna arbetar som konsulter och precis som de själva säger så har de goda kunskaper inom teknikområdet och är på så sätt medvetna om vad de gör och vilka konsekvenser detta kan få. De båda använder även utbildning som ett medel för att sprida information både till nyanställda, gentemot de kunder som de arbetar med men även sina anställda i vissa fall. Utbildning anses vara den metod som fungerar för att minska den mänskliga felfaktorn. De båda företagen använder sig av tydliga regler och policys och har en IT-säkerhetspolicy, dels för att minska mänskliga fel men även för att säkerställa de logiska aspekterna i form av lösenord och dess hantering. Mitrović (2005) påpekar och styrker vikten av människor och processer i datasäkerhet, där han anser att god datasäkerhet är 80 procent människa och processer. MOROTSmedia har en stark hotbild på den fysiska sidan och detta gör att de har satsat mer på denna del än på andra säkerhetsaspekter för att upprätthålla en god och samtidigt reell datasäkerhet på detta område. Det stora hotet är inte att någon är intresserad av den information de har utan deras utrustning. Detta har gjort att de har installerat pansarglas, har låsta dörrar och tydliga riktlinjer och regler för hur informationen lagras, hur man hanterar bärbara datorer, hur arbetsplatsen ska se ut när man lämnar den för att inte skylta med att där finns värdefull utrustning men även rutiner som gäller dörrar och lås för att skapa en säker miljö. MOROTSmedia har även tekniska lösningar för att stänga ute elektroniska inbrott och denna registrerar ett visst antal försök men det är inget utöver det normala och heller inget som de inte klarar av. Då båda företagen arbetar med konsultation anser de sig vara kunniga inom datasäkerhet och på detta sätt har de också en högre nivå på sitt sunda förnuft i jämförelse med många andra företag. Detta innebär att de båda företagen har en god uppfattningsförmåga för olika risker som kan uppstå genom att utföra en viss handling. Detta innebär även indirekt att de båda tidigt kan undvika faror som kan uppstå.

Vi anser att de båda företagen skyddar sig på ett tillfredställande sätt i relation till deras individuella hotbild. De båda företagen har bidragit med tillräckligt mycket information för att vi ska kunna besvara forskningsfrågan och kunna ställa de båda företagen i relation till varandra. Däremot har vi fått mer ingående information av MOROTSmedia på grund av respondenten var mer öppen än konsulten på Atea i Sverige. Då de är konsulter och interagerar med många kunder och även därmed många säkerhetslösningar bedömer vi att deras egna säkerhetsarbete håller en hög nivå. De båda företagen arbetar som konsulter och hämtar nya erfarenheter hos nya kunder, bearbetar dessa och i framtiden kan de då även applicera lösningar eller förslag hos andra kunder. Denna position gör att de båda företagen erhåller information och inspiration från kunder och därmed skapar sig en hög datasäkerhetsmedvetenhet.

6. Slutsats

6.1. Slutsatser

De värderingar eller fördomar vi hade innan studien startade var att det större företaget skulle ha en högre datasäkerhetsmedvetenhet på grund av storleken och den möjliga ekonomiska fördelen gentemot det mindre företaget. Vi trodde även att de mindre företagen skulle vara fokuserade på sin uppgift och därmed glömma bort datasäkerheten, eller på sin höjd använda sig av sunt förnuft som säkerhetslösning. De fördomar vi hade bekräftades när vår första intervju var gjord med Atea i Sverige då dessa hade hög medvetenhet när det gällde datasäkerhet och arbetade med detta som huvudsyssla i form av konsultation. Detta gjorde att vi började fundera på om de var medvetna på grund av sina arbetsuppgifter eller för att de var ett stort företag. Konsulten på Atea i Sverige delade med sig om både hur de själva arbetar, med begränsad detaljrikedom, men även hur de arbetar med sina kunder. Anledningen till den begränsade information som vi fick av konsulten kan bero på att han inte var insatt i hur det egna företaget i sin helhet ställde sig till datasäkerhet utan kunde endast referera till sina egna värderingar och uppfattningar kring ämnet. Efter att ha utfört den andra intervjun med det mindre företaget, MOROTSmedia, kunde vi ställa de båda företagen bredvid varandra och jämföra deras datasäkerhetsmedvetenhet. MOROTSmedia hade en högre säkerhetsmedvetenhet än vad vi förväntade oss, då de hade god kontroll på policys, rutiner och diverse säkerhetslösningar som de med glädje delade med sig av under intervjun med oss. De båda företagen anser sig själva ha en god datasäkerhetsmedvetenhet dels för att de båda bedriver konsultverksamhet som berör både IT och säkerhet men även för att de är tekniknära företag med en stor andel anställda som är teknikkunniga .

Den forskningsfråga vi hade inför denna studie var hur två svenska IT-företags datasäkerhetsmedvetenhet såg ut och hur de skyddar sig i förhållande till deras verksamhet och dess storlek. Vi anser, precis som de själva hävdat, att de båda företagen har en hög datasäkerhetsmedvetenhet då de båda har utformat policys, rutiner och olika processer för att upprätthålla den önskade datasäkerheten i företagen i förhållande till den hotbild finns mot företaget. De båda företagen är av olika storlekar och har anpassat sin datasäkerhet efter de behov och hotbilder de står inför och detta är ett tecken på säkerhetsmedvetenhet hos företagen. Anledningen till denna medvetenhet anser vi inte vara storleken på företaget utan hur viktig data som företagen lagrar i relation till hur viktig denna data är för andra, såsom konkurrenter eller andra intressenter. Självklart spelar storleken roll i vissa avseenden då större företag vanligtvis har större ekonomiska resurser för att upprätthålla och underhålla diverse säkerhetslösningar. Utan säkerhetsmedvetenhet kan dessa ekonomiska resurser spenderas på säkerhetslösningar som inte gynnar företagets datasäkerhet på ett effektivt sätt. För att uppnå en effektiv datasäkerhetslösning behöver organisationer investera i rätt typ av säkerhetslösningar för att skydda en viss typ av data på ett önskvärt sätt och lösningen på detta är inte enbart pengar. Vi anser även att företagets verksamhetsområde spelar en stor roll i deras säkerhetsmedvetenhet då vissa företag har teknik som huvudområde och har därmed ett tekniskt försprång jämfört med andra företag som får ta hjälp av andra företag utanför organisationen. Då vi har valt att undersöka två företag inom liknande verksamhetsområde där företagen både är tekniskt orienterade samt bistår med kunskap till andra företag så kan vi styrka detta. Sammanfattningsvis anser vi att datasäkerhetsmedvetenhet inte är beroende av företagets storlek eller någon ekonomisk mångfald utan det handlar om hur viktig information man lagrar, både för sig själv och för andra företag

eller intressenter. Då information kan vara mindre viktig för sin egen verksamhet behöver inte det betyda att informationen är mindre viktig även för andra företag och intressenter. Det är därför viktigt att informationen skyddas på ett adekvat sätt så att rätt typ av säkerhet appliceras – rätt skydd, på rätt plats, mot rätt personer.

6.2. Reflektioner

Kunskap är källan till allt som man är bra på eller vill bli bättre på och vårt val att intervjua två teknikorienterade företag som har goda kunskaper inom datasäkerhet, kan vara anledningen till att företagen inte skiljer sig så mycket inom detta ämne. På grund av företagens verksamhetslikheter men också intervjupersonernas arbetsuppgifter blev svaren på våra frågor snarlika. En skillnad mellan företagen är att vi antar att vi hade fått samma svar från vem som helst av de anställda hos MOROTSmedia till skillnad från Atea i Sverige. Atea i Sverige är ett mycket större företag och det blir därmed väldigt svårt för alla anställda att ha samma kunskap om datasäkerhet eller lika bred kunskap som vår respondent hade. Om vi hade intervjuat en säljansvarig på Atea i Sverige så hade resultaten på intervjun antagligen sett väldigt annorlunda ut, dock så hade detta också lett till mindre ingående information om datasäkerhet på grund av mindre kunskap hos denna respondent. Vi kan här ställa oss frågan om det är viktigt att se hela företagets syn på datasäkerhet och hur datasäkerhetsmedvetna de är istället för att intervjua en väldigt kunnig person i företaget vars arbetsuppgifter kretsar kring datasäkerhet. Vi anser att det hade varit intressant att se hur datasäkerhetsmedvetenheten såg ut hos personer med andra roller i företagen men vi menar också att vår undersökning ger en god inblick i hur medvetna företagen är om datasäkerhet gentemot sig själva och sina kunder.

Vi anser att om man verkligen vill förstå hur medvetet ett företag är gällande datasäkerhet så måste intervjuer utföras och därefter tolkas. Att genomföra studien med blanketter eller liknande empiriverktyg hade gett oss tiden att undersöka fler företag men vi hade inte fått någon insikt över hur medvetna de egentligen är. På grund av att datasäkerhet är en känslig fråga för många företag så måste undersökningen genomföras på ett förtroendeingivande sätt. Frågor gällande datasäkerhet kan vara svåra att planera och formulera på grund av dess känslighet men också att datasäkerhet skiljer sig mycket från företag till företag. I dagens svenska samhälle är brandväggar och antivirus en självklarhet för många som använder datorer och IT. Därmed insåg vi när vi före intervjuerna skapade en intervjuguide att frågor angående brandväggar och antivirus inte är givande när man intervjuar två väldigt teknikorienterade företag om datasäkerhetsmedvetenhet.

6.3. Framtida forskning

Vidare hade det varit mycket intressant att undersöka medvetenheten om datasäkerhet hos ett företag som använder IT men inte arbetar med det i form av utveckling eller konsultverksamhet. Ett företag som inte är lika tekniskt orienterade gentemot IT hade kanske gett en annan syn på datasäkerhetsmedvetenhet, där till exempel sunt förnuft är den främsta faktorn för god datasäkerhet. Vi anser därmed att det hade varit mycket intressant om framtida forskning tar upp ämnet och undersöker aspekter som inte vi har belyst. Att undersöka mer än två företag hade varit bra för att till större grad säkerställa vårt resultat, det vill säga att vi tror att resultatet inte hade varit väldigt olika om fler företag inom samma verksamhetsområde, hade varit med i undersökningen.

Referenser

Bace, R. G. (2000). *Intrusion Detection.* Indianapolis: Macmillan Technical Publishing.

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

Bernard, R. (2007). Information Lifecycle Security Risk Assessment: A tool for closing security gaps. *Computers & Security* (26), 26-30.

Brottsförebyggande rådet. (den 30 mars 2007). *Brottsstatistik/2006*. Hämtat från Brå - Brottsförebyggande rådet - 2006: http://www.bra.se/extra/pod/?action=pod_show&module_instance=8&id=46&statsType=100&statsCounty=La&Year=2006&type=1 den 1 april 2007

Bryman, A. (2002). *Samhällsvetenskapliga metoder.* Trelleborg: Liber AB.

Davies, D. (2006). Data security. *Canadian Mining Journal , 127* (3), 9.

Jones, A. (2007). A framework for the management of information security risks. *BT Technology Journal , 25* (1), 30-36.

Kilcourse, B. (2005). Rethinking Data Security. *Chain Store Age , 81* (2), 47.

Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., & Morrow, D. W. (2006). The Top Information Security Issues Facing Organizations: What Can Government Do to Help? *Information Systems Security , 15* (4), 51-58.

McCumber, J. (2005). *Assessing and Managing Security Risk in IT Systems.* Boca Raton: Auerbach Publications.

Mitrović, P. (2005). *Handbok i IT-säkerhet* (4:e uppl.). Falun: Pagina Förlags AB.

Panko, R. R. (2003). *Business Data Networks and Telecommunications.* New Jersey: Prentice Hall.

Panko, R. R. (2004). *Corporate Computer and Network Security.* New Jersey: Prentice Hall.

Pastore, M., & Dulaney, E. (2006). *CompTIA Security+ Study Guide* (3rd ed.). Indianapolis: Wiley Publishing, Inc.

Pfleeger, C. P., & Pfleeger, S. L. (2003). *Security in Computing* (3rd ed.). New Jersey: Prentice Hall.

Polaniecki, R. (2006). A Blueprint for Security. *Credit Union Management , 29* (2), 42-45.

SCB. (den 15 Januari 2007). *Andel företag som använder datorer efter storleksklass och bransch.* Hämtat från Statistiska Centralbyrån: http://www.scb.se/templates/tableOrChart____28117.asp den 28 Maj 2007

SCB. (den 15 Januari 2007). *Andel företag som använder olika säkerhetsanordningar*. Hämtat från Statistiska Centralbyrån: http://www.scb.se/templates/tableOrChart____112431.asp den 28 Maj 2007

Scheraga, D. (2006). Data Security Is A Physical Issue, Too. *Chain Store Age , 82* (2), 54.

Stallings, W. (2003). *Cryptography and Network Security* (3rd ed.). New Jersey: Prentice Hall.

Stallings, W. (2002). *Network Security Essentials*. New Jersey: Prentice Hall.

Tittel, E., Hudson, K., & Stewart, J. M. (1999). *Intensivplugga Networking Essentials* (3rd ed.). Sundbyberg: Pagina Förlags AB.

Wallström, P. (den 5 juli 2005). *Mörkertalsundersökningen 2005: Svenska organisationer om IT-säkerhetsincidenter*. Hämtat från Post & Telestyrelsen: http://www.pts.se/Archive/Documents/SE/Morkertalsundersokningen_2005.pdf den 1 april 2007

Bilagor

Bilaga A: Underlagsfrågor till intervju

Hur många anställda är Ni på **** och hur många av de anställda har en dator som interagerar med nätverk/internet/företags-/kundinformation?

Hur är Er generella syn på datasäkerhet? (fysisk, logisk, mänsklig)

Vilken typ av säkerhet prioriteras och hur/var implementeras denna?

Är ni väl medvetna om riskerna som finns och anpassar det skydd Ni använder Er av mot det hot som eventuellt kan uppstå?

Är Ni ett företag som ofta bli utsatta för hot?

Vad är det värsta som enligt er kan hända gällande datasäkerhet?

Vilken typ av data är det Ni önskar skydda? (mycket viktig information eller ett generellt skydd)

Hur arbetar Ni för att upprätthålla den säkerhetssynen?

Hur arbetar ni för att säkerställa den mänskliga riskfaktorn?

Har personal och ledning en delad uppfattning om de säkerhetsprinciper som finns?

I de tjänster ni utvecklar/säljer, har ni applicerat er eller kundens säkerhetsfilosofi?
…och hur tillämpas ni denna?

Bilaga B: Transkribering av intervju med MOROTSmedia

Intervjuare	Daniel Berntsson och Oskar Grunning
Datum för intervju	2007-05-15
Intervjulängd	40 minuter
Företagets namn	MOROTSmedia
Intervjuad person	Filip Strandqvist
Intervjupersonens position	VD, konsult
Plats för intervju	MOROTSmedia

DO är intervjuarna Daniel och Oskar *IO är intervjuobjektet hos MOROTSmedia*

DO: Då börjar vi med en fråga angående generellt vad ni sysslar med, hur många anställda ni är…
IO Asså, ja, det kan vi göra. Jag jobbar, vi är en lite koncern av en liten grupp företag där ett bolag är, som ni har hittat mig på, MOROTSmedia som är ett eget konsultbolag som jobbar med systemutveckling och programvaruutveckling på kontrakt. Vi är fem personer. Sen har vi ett bolag som heter Distributed Medicals som jobbar med medicintekniska system, det är lite det ni ser uppmonterat här inne, det här är egentligen ett demorum för dem slash konferensrum. Som gör system för bild- och ljudupptagning för operationsmiljöer, konferensverktyg för röntgen, kliniker och andra relaterade liknande system – datainsamlingssystem och så vidare. De är sex personer. Det är vi och dem företagen som delar den här lokalen. Sen har vi en bredbandsverksamhet som heter Perspektivbredband som sitter en våning upp i en ungefär likadan lokal, den är lite djupare, och dem är tjugofem personer. Jag är anställd i MOROTSmedia, det är, vill säga, mitt arbete som jag konsult i. Jag jobbar mycket internt med våra andra verksamheter så en hel del av mina uppdrag ligger vill säga inom gruppen - affärsutveckling och den lite mer administrativa typen av uppdrag.

DO: Och datasäkerhet om vi ska gå dit då. Hur din eller er generella syn är på datasäkerhet.
IO: Alltså datasäkerhet i vår värld kan ju vara till exempel i konsultbolaget så handlar datasäkerhet mer om att skydda den information som bolaget har, antingen är den känslig för vårt villkor eller så är den känslig för kundernas villkor. Vi sitter ju med en massa information från våra kunder som inte under några omständigheter får lämna huset här så att säga – VPN uppkopplingar till olika sjukhusnät, Tetra Pak, Sony Ericsson och sånt som göra att vi kan nå mycket information hos dem. I dem sammanhangen så handlar datasäkerhet mycket om att se till att rätt människor har tillgång till rätt information, eller inte har tillgång till information, och att man har väldigt goda administrativa rutiner, hur man hanterar lösenord, hur man hanterar in- och utloggningar, hur man segmenterar nät alltså vilka datorer du faktiskt sitter inkopplad i och vilka nätverk. Och inte så mycket om det rent tekniska datasäkerhetstänket, i många fall handlar datasäkerhet för en konsultverksamhet om att leva upp till kundernas säkerhetspolicy och säkerhetstänk – hur man bibehåller dem när man får in deras miljö i ens egen utvecklingsmiljö. Så att i de två verksamheter som sitter här nere så är det ju i huvudfokus, tittar man senare på om man ställer samma fråga till han som är nätchef för bredbandsverksamheten där uppe så kommer han börja prata om routing, IP-filtrering, den typen av segmentering, isolering av nätsegment och trafikflöden och så där – för att se till att deras produkt, bredbandsaccess, är stylad på ett sätt så att kunden inte behöver tänka på det så mycket själv. Så att datasäkerhet är lite olika beroende på

vem man frågar men det är ju så klar något vi tycker är viktigt som… Vi har ganska hög datasäkerhetsmedvetenhet inom vår verksamhet för att vi är så teknisktorienterade.

DO: Finns det någon typ ni prioriterar högre än något annat?
IO: Ni får nog specificera frågan mer… Ge fem exempel på typer (skratt)

DO: Du nämnde det här med, alltså informationen ni skyddar bättre än annat VPN uppkopplingar och så vidare. Finns det några andra punkter som känns att dem är… Att de bör skyddas med de skyddas inte lika hårt som just de här viktiga uppkopplingarna och datan.
IO: Alltså helhetsbegreppet på datasäkerhet är ju egentligen det som är det viktiga, det är lite som det där gamla tugget som att ingen kedja är starkare än sin svagaste länk. Men… en sak som vi till exempel gjorde när vi flyttade in i den här lokalen var att vi bytte till pansarglas i alla fönster – om man kan kalla det datasäkerhet är väl kanske tveksamt men man kan ju skydda sig hur mycket som helst med lösenord och så vidare, och vara noga med det, men om man sen har en fysisk miljö som är väldigt lätt att ta sig in i och stjäla ifrån, jag menar, kommer de in här och tar en dator så kan man extrahera det mesta ur en dator utan något lösenord, det är ju en enkel manöver. Så att just att ha ett helhetsgrepp är prioritet nummer ett, att man inte är petnoga i vissa avseenden och sen att man bortser från andra avseenden, som till exempel fysisk säkerhet eller att man alltid stänger ytterdörren att man inte låter den stå på vid gavel för att det är bekvämt när man springer in och ut, vi springer rätt mycket emellan planen, för rätt som det är så vandrar det in någon annan människa som inte alls har med vår verksamhet att göra och som när det är lite folk här, det är rätt lite folk här över lunch och så, drar han med sig någons laptop eller någonting. Det är rätt mycket sådana problem som har varit här på Ideon periodvis så att, jag tror att man ska ha en rimlig men jämn nivå, en ganska grundläggande filosofi när det gäller datasäkerhet.

DO: Är det så att ni blir utsatta ofta för hot som ni vet om?
IO: Jag tror att intresset för att stjäla information ifrån något av våra bolag är ganska lågt, jag tror inte att vi är ett typföretag som man gärna vill ”hacka” och stjäla information ifrån. Jag tror det största reella hotet vi har här är just att de bryter sig in och stjäl datorer och därmed information men inte för han egentligen ser informationen men han vill ha den här TV:n hemma eller något åt det hållet. Men sen till exempel den här som har datorn till skärmen ligger femtio filmer på hjärtoperationer som han kanske egentligen skiter fullständigt i, han kommer bara att formatera disken och installera Windows XP Media Center på den och vara glad. Men det är ju information som till exempel från sjukhusets perspektiv är extremt känsligt, så att det är också en fråga hur stor hotbilden egentligen är. Det skulle vara hemskt bekymmersamt för oss om vi skulle bli av med den men han som stjäl den kanske inte funderar alls på vad det är i den och formaterar den direkt för att röja alla spår kring en stöld eller något åt det hållet. Så det är svårt att svara på frågan jag tror den största reella hotbilden, inte är industriella spioner eller någon som faktiskt vill anstränga sig för att stjäla information, det är den som stjäl informationen för att stjäla något annat. Tittar man på intrångsservers och sånt som brandväggar och så är det ju nästintill obefintligt. Det förekommer ju lite DDoS attacker och så, som förekommer hela tiden, robot som portskannar för att slå ut saker med den typen av attacker. Den typen av trafik får vi in här på nätet hela hela tiden. Men vi ser inte det som ett reellt hot för vår datasäkerhet.

DO: Policys och så där inom företaget… finns det något?
IO: Det finns… I vårt fall så är det inte en särskriven utan respektive bolag har ett kapitel i sin personalhandbok som handlar om IT-säkerhet. Och det är rätt så snarlikt, det handlar mycket om att man ska… den information man har tillträde till genom sin anställning är man också förpliktigad att skydda på ett förnuftigt sätt. Ungefär så, det står inte exakt så men det är meningen med det som står där. Att man inte får lämna sin PC utan att låsa… skärmen och… att

man inte får kopiera en massa saker ner på USB stickor och ta med den hem för att det är så smidigt och så vidare. Vi ger lite tumregler för hur man bör och inte bör hantera informationen, sen om någon faktiskt tar en USB sticka och tar hem en massa information det är ju inget vi kan kontrollera.

DO: Hur är det med lösenordshantering och?
IO: Vi har normal lösenordsrotation, kryptering och en form av minimum krav - åtta bokstäver, siffror måste finnas med, vissa bokstäver måste vara gemena och vissa måste vara versaler. Traditionell lösenordshantering, jag tror vi använder Microsofts Password Template, förmodligen.

DO: Vad är det värsta enligt er som kan hända gällande datasäkerhet? Men det har vi redan gått in på lite med stöld kanske?
IO: Det är ju det som är mest reellt men det värsta som kan hända är att man fick ett reellt inbrott, alltså ett nät mässigt inbrott, där de kopierade mängder av information för att han har glädje av den informationen. Jag har väldigt svårt att föreställa mig det att det är något företag som har glädje av MOROTSmedias information, det skulle i så fall vara ett bolag som konkurrerar head on emot oss – som hade exakt samma kunder och som ville veta vad vi gjorde exakt just nu. Information har nämligen en tendens att bli i stort sett värdelös så fort den blir snabbt gammal, en offert som vi lämnade till Tetra Pak för två år sedan är det ju ingen som är intresserad av men en offert som vi lämnade igår kan någon vara väldigt intresserad av. Det är väldigt begränsat med information som vi har som kan vara till värde för någon annan. Det som skulle kunna anses vara ännu värre det är att någon stjäl information ifrån oss som inte är vår… vi sitter kanske med ett stort utvärderingsprojekt eller något hos Tetra Pak där vi har fått en massa dokumentation ifrån dem som på något sätt ska byggas in eller importeras i det här systemet som vi bygger och att sen någon stjäl den, det skulle vara ett tråkigt och trist scenario att behöva gå till. Att gå till Tetra och säga ”Hej, vi… på grund av bristande datasäkerhetsrutiner så har någon stulit information bland annat er information, vi har ingen aning om vem och vi kan bara beklaga och hoppas att ingenting händer” det skulle vara hemskt tråkigt och det skulle ju kunna få ekonomiska konsekvenser. Men ärligen så är det inte något som vi går och funderar så mycket på, vi har ju som sagt ett adekvat skydd för den data vi hanterar och vi har ingen verksamhet av den arten där det skulle finnas ett jätte intresse.

DO: Men… när ni arbetar som konsulter jobbar ni direkt med datasäkerhet?
IO: Det gör vi en del men vi sitter inte och installerar brandväggar och antivirusprogram. Men vi är ganska ofta med dels när man implementerar, vi bygger ju system i grunden och en del är att bygga och implementera systemet för en extern part innebör ju att man tillförsäkrar att det här systemet även är säkert att man bygger in adekvata säkerhetskontroller i systemet – normalt sätt när man levererar ett system för ett stort företag så kräver de att, för att man överhuvudtaget ska kunna starta applikationen, man måste logga in i applikationen så att inte vem som helst hos dem… för dem har ju inte heller en perfekt värld i sitt nät… så de lätt kan kontrollera lätt vem som i deras egna miljö ska använda applikationen. I väldigt många fall när man jobbar med stora bolag så bygger man… där dem lägger upp fem användare på den databasen… vi har 140000 anställda och ni ska integrera emot den och hitta de här flaggorna, vi kommer sätta en flagga som heter access. Om den anställda har den rätta accessflaggan då får den starta applikationen. Sen måste man ta hänsyn till om vårt system ska kommunicera med ett annat system, att den kommunikationen tillkommer på ett säkert sätt. Att den inte sker i klartext utan efter en viss standards som dem har certifierats som… systemkommunikationsstandard… den datasäkerhetsaspekter som dem redan ska ha, att man följer den typen av datasäkerhet. Det kan vara en typ av datasäkerhetsarbete man gör som konsult, en annan kan vara att man gör rena

datasäkerhetsjobb… de kommer till konsulten och säger ”Vi har den här miljön och vi har problem med säkerheten kan ni hjälpa oss att titta på lösningar där vi kan höja säkerheten med avseende på individuell kontroll eller access”. Det kan ju vara så att vi föreslår utbildning av personalen i slutändan för att personalen verkar helt sjövilda det kan ju vara en lösning. Och ibland kan det vara så att man anser att de borde köra den här… kryptera era hårddiskar och så vidare… Det kan ju alltså också vara en teknisk lösning på kundens problem. Men väldigt ofta så handlar det om att hitta nya rutiner hos kunden för att höja säkerhetsmedvetandet helt enkelt.

DO: Då går ni in och hjälper till med policys och liknande då också eller?
IO: Ja precis, då skriver man det tillsammans med kunden och oftast är det ju den som är ansvarig för IT avdelningen som kanske inte alls vet så mycket om datasäkerhet och som just behöver något att komma in… han skriver sin problemsituation… man bekräftar den och det kan till exempel vara att vi säger att det är rutinmässiga lösningar eller tekniska lösningar som kan lösa problemsituationen. Ger dem en kostnad för att jobba igenom problemet och sen accepterar man det och därefter producerar man då något som till exempel rutin- eller processmässiga lösningar. Och det kan ju vara att man skriver en handbok… handbok i datasäkerhet för Tetra Pak… sen så distribuerar man den och kanske håller några workshops med personalen där man går igenom den handboken, lär dem och utbildar dem i varför det är viktigt och varför man ska tänka på detta… vad det kan få för konsekvenser om ni inte tänker på detta… att ha den typen av dialog med personalen.

DO: Finns det några skillnader emellan personal och ledning här eller vad du har sett ute som konsult – har du sett någon skillnad vad de tycker är vikigt eller vad de prioriterar?
IO: Nja, här internt så har vi, vi har en väldigt platt organisation, det finns inte direkt ledningsgrupper och fotfolk utan alla verkar så samma nivå men om man tittar på till exempel ett bolag som IKEA eller Tetra Pak då har man ju en mängd olika nivåer i organisationen… Jag tror inte man kan säga något generellt att ledningen inte fattar någonting men de anställda brukar veta eller tvärtom men däremot är det ju alltid så att när ett behov uppstår… det är ju aldrig så att en anställd på Tetra Pak ringer till mig och säger till mig ”Du, du brukar ju vara här som konsult… Kom hit för vår datasäkerhet suger”. Det initiativ som kommer till oss kommer ju i princip alltid ifrån ledningen… ”Vi har identifierat det här när vi har tittat på det här… om detta, detta och detta… där verkar det vara en brist i säkerheten och vi behöver se över det här… kan ni göra detta tillsammans?”… Den typen av initiativ kommer ju alltid i princip ifrån en slags ledning… det kan ju vara att det ringer någon divisionschef ”jag tycker att våra anställda inte fattar någonting – vi måste sätta in ett mycket säkrare system”… oftast är det ju så att något har hänt att en PC har blivit stulen eller någonting och så triggar det igång den där processen. Shit vi måste ha bättre datasäkerhet. Ibland är det så att de tror att de måste ha bättre datasäkerhet och att det är lösningen på problemet men ibland är det inte alls det som är lösningen på deras problem, så ibland måste man hjälpa dem att identifiera det istället för att försäkra en bättre datasäkerhet. Så, var problembilden ligger skiljer sig väldigt mycket med initiativet kommer oftast från ledningsnivå.

DO: Hur är det med etiska hot som till exempel rasdiskriminering, spam-mail och mail av sexuell natur eller liknande? Hur?
IO: Spam är ju en rätt så hanterbar problematik idag, det finns rätt bra lösningar… det är ju ett problem som man löser med tekniska verktyg. Spam går inte att undvika utan det är något som man får hantera i den takten den kommer in och med den mjukvara man i regel applicerar på mailservern. Jag vet bredbandsverksamheten som har väldigt mycket e-post konton som de håller för sina kunder sorterar bort ungefär en miljon spam om dagen. Det identifieras ju innan det läggs i en mail box… så gör man en identifiering, då har man ett rating system oftast som tittar på brevet och beroende på vad det är för avsändare, mottagare, ämne, vilken mailserver det har

kommit igenom eller vilket nät det har kommit ifrån, innehållet och mixen av innehållet, färger och så vidare får olika poäng och om det då kommer över en viss poäng i detta rating system så anses det då vara spam och då bara slänger man det. Sen slänger man säkert vissa felaktiga och legitima mail med det får man ju acceptera. Graylisting är ju en annan teknologi som löser ganska mycket av spammen, när man får ett mail hit och inte har fått något av den avsändaren innan så bounce:ar man mailet och säger ”system busy” och om då avsändaren är en riktigt avsändare så får hans mailserver denna bounce:en och säger ”då skickar jag igen om en liten stund”, den brukar väl ha en delay på ungefär 600 sekunder, och så skickar den mailet igen… får man det då igen så accepterar man mailet och därefter så testar man mailet för att se om det kan vara ett så kallat spam mail vilket det ibland fortfarande kan vara. Men i de allra flesta fallen så kräker man bara ut fem miljoner mail och får man sen tillbaka lite bounce:ar så skiter man i det… man använder ju vanligen inte ens en riktigt e-postadress utan en fake:ad eller en icke existerande adress. Så det gör att när man väl bounce:ar så med hjälp av graylistingteknologin så är det ingen som håller på med spam som tar hand om det och skickar det igen om fem minuter. Så på den sidan finns det väldigt bra tekniska lösningar på problemet. När det gäller sexuella trakasserier så vet jag inte riktigt vilken koppling det har med datasäkerhet kan ha…

DO: Nej men det är väl mer som… IT kan ju vara ett medel… att det kan komma mail som har ett innehåll som…
IO: Aha, som att man till exempel trakasserar en kollega genom att skicka mail till dem då?
DO: Ja eller att det kommer utifrån… det kan vara propaganda som är illariktad emot en viss ras eller kön…
IO: Jag har faktiskt aldrig… Naturligtvis kan det ju vara så, precis som du säger. Vi får säkert politisk propaganda genom massutskick precis som allt annat som massutskickas men jag har aldrig varit med om en affärsmässig situation där ett bolag har kommit till oss och säger så här att ”vi har problem med det här specifika” som har med sexuella trakasserier eller annat förtryck att göra. Jag har varit med om att enskilda individer på ett företag har förtryckt andra individer inom företaget via just mail eller datorsystemen. Men lösning på det är ju oftast inte att skapa ett slags system eller en kontrollmekanism kring… skickas det mobbningmail eller inte i systemet idag… utan lösningen är ju oftast att den som är mobbad går till sin chef och säger att ”Ja, han Nisse där… han skickar oanständiga mail till mig” och sen löser man det genom att prata med Nisse och säger ”Nu får du sluta med det här för annars kan du inte jobba här” också slutar han förhoppningsvis med det. Då hanterar man ju det på det sätter, det är ju oftast personalavdelningen som hanterar sådana frågor. Jag har väl varit med för att just identifiera någon av dem som skickar mail… för att kolla vem det egentligen är som skickar de här mailen… Man hade väl misstankar men man ville väl vara helt säker innan man gick till den personen och anklagade den för det här och säga till den att sluta. I några sådana situationer har jag varit med och hjälpt till och då har jag just varit där för att tillförsäkra att det är han som gör det här. Men som sagt, hanteringen av något sånt där när det väl är uppdagat och överbevisat sköts ju av en annan typ av människor på företaget.

DO: Hur är det begränsningar och kontroll av personal för till exempel ett större företag?
IO: Du menar att man typ så här… Man kontrollerar dem och spärrar vilka webbsidor de kan komma åt… vad man kan maila privat och så?
DO: Precis.
IO: Det är väl lite olika. Generellt kan man säga att amerikanska företag tenderar att vara väldigt mycket striktare i jämförelse med svenska företag. Banker tenderar också att vara väldigt strikta. Vi har jobbat en del med Trygg Hansas bankverksamhet i Stockholm, det är några år sedan nu så det är inte direkt jätteaktuellt men de hade problem med… de kontrollerade ganska rigoröst vem och var folk surfade och sedan skapade de topplistor på, inte över vem som surfade var men var det surfades, och så såg dem ju då att det surfades väldigt mycket till Aftonbladet, Dagens

Industri och ett antal andra media tunga sidor av det slaget… och sen vid något tillfälle så ploppade det då upp något sånt här Lunarstorm, så någon månad så hade man väldigt hög aktivitet på Lunarstorm och då fick vi… själva listan producerades ungefär en gång i månaden och skickades till någon typ av IT chef eller så… och då fick vi vid något tillfälle tillbaka den och de sa ”Ja, nu har den här seglat upp som fyra och det är inte okej”. Så det var en godtycklig grej… det var okej att surfa på Dagens Industri eller Aftonbladet men det var inte okej att surfa på Lunarstorm tyckte man då där… Så ville de veta vem och om det finns några speciella individer som gör det här eller är det en massa människor som gör det här och så tittade vi på det då… och i det fallet så var det ett par individer som hade ganska hög aktivitet just på den här sidan och det rapporterades sedan tillbaks men det hanteras ju precis som jag sa innan, det behandlas sen av någon annan på ett mer personalrelaterat sätt. Men jag skulle faktiskt vilja påstå… integriteten är rätt så hårt skyddad i lagen i Sverige… man får ju inte lov att lyssna eller läsa folks mail hur som helst utan då bryter man mot lagen så att säga. Så att svenska företag har nog en kultur av att inte vara snokande eller… man litar helt enkelt på sin personal… amerikanska företag är däremot lite mer kontrollfreaks, de har system där det ringer en varningsklocka om något går utanför mönstret och så tittar de på det från fall till fall. Men jag har ingen jätteerfarenhet av det… dock så är min gissning att det generellt sätt är så och sen finns det ju säkerligen svenska företag som är fullkomliga kontrollfreaks, det gör det säkert. Vi bedriver inget sånt… kontroller över anställda för att kolla vad de sysslar med eller inte… om det inte är så att det uppdagas här… jag vet att någon i supporten hos bredbandsverksamheten inte gjorde, skötte inte sina sysslor på jobbet helt enkelt och då började man fundera på vad människan gör här åtta timmar om dagen… då vet jag att man tittade på till exempel vad för sidor den här människan och vad för typ av trafik och det visade sig att han satt och IRC:ade sex timmar om dagen… man kollar ju inte på vad utan konstaterar bara på att IRC protokollet är flitigt använt från det IP numret. Det är nog mer på den nivån i svenska företag när något inte verkar stå rätt till, då kanske man tittar bland annat på vad vederbörande använder sin dator till.

DO: Hur arbetar ni för att upprätthålla datasäkerhet och säkerhetsmedvetande… både här och gentemot andra företag?
IO: Internt… i den här koncernen så jobbar vi med information där nyanställda får en mindre föreläsning om en massa saker däribland datasäkerhet. Sen är det hos oss, precis som hos många andra, när det händer någonting att till exempel en säljare har sin notebook, att han lämnar den i bilen och att det blir inbrott i bilen. Någon gång om året så kanske det händer någon sådan grej och då brukar det uppdagas det här… och någon tar på sig moralhatten och går ut för att berätta för alla ”Tänk nu på detta, detta, detta och detta. Man gör inte så här och man lämnar inte sin dator och så vidare”… Det är något som alla redan vet men som, just för att repetera det. Utåt… vi säljer ju inte oss som ett datasäkerhetsföretag utan vi bedriver ju datasäkerhetskonsultation på anmodan av externa kunder, vi säljer oss som ett systemutvecklingsföretag vilket gör att vi jobbar väldigt väldigt lite aktivt utåt med datorsäkerhet. Det finns ju företag som har den profilen, som sin huvudsakliga näring, men det har inte vi.

DO: Ska vi se om vi har någon fråga kvar – Det tror jag inte riktigt…
IO: Var det som ni trodde? Ni måste ju ha haft en bild av oss här, någonting fick er att komma hit liksom. Blev bilden besannad?
DO: Nej, det skulle jag faktiskt inte riktigt säga. Jag trodde det skulle vara lite mer sunt förnuft än vad det faktiskt var. Ni är ju ett mindre IT företag om man till exempel jämför med Atea…
IO: Jag tror så här när man har en organisation som har ganska mixad personal då får man jobba mer med sunt-förnuft-faktorer… Vi fem som jobbar på MOROTSmedia vi är liksom IT nördar allihopa, så att bara säga att sunt förnuft duger för oss blir lite tafatt för vi är allihopa väldigt medvetna om datasäkerhetens vikt och dess upp- och nersidor. Så utan att anstränga sig så kan vi ha lite högre krav och tänka ett steg längre för att vi just sitter på kunskapen. Men om man ser på

Atea som har 800 till 1000 anställda så skulle jag gissa att inte mer än 200 har hyfsad koll på datasäkerhet, 200 administratörer… säljare och sådant. Så de har ju en stor grupp där datorsäkerhet kanske inte sitter i bakhuvudet utan där det mer kanske är ett begrepp. Ännu hellre titta på ett företag som Tetra Pak eller något sånt som använder IT var tredje sekund i sitt arbete men som inte är ett IT företag för det, där får man ju ha rutiner som bygger mer kring sunt förnuft – allting bygger ju egentligen kring sunt förnuft men anledningen till att man gör på ett visst sätt kan ju optimeras om man har kunskapen också och det tror jag vi tillämpar mycket.

DO: Min bild av det byggdes upp av att jag ringde runt till andra mindre företag här på Ideon och det var ju väldigt många gånger svar, för jag nämnde det med policys och datasäkerhet, och det var många som sa att de inte alls hade några policys och att de bara går efter sunt förnuft och därav att de inte var ett bra intervjuobjekt. Så det var väl därför jag skapade mig den synen.
IO: Och det är säkert… jag tror inte Ideon är ett särskilt bra intervjuoffer för en sån här grej för de flesta bolagen här de är inte i en kommersiell strukturerad fas… Ideon har ju nästan 200 bolag nu och jag tror att 180 av dem är ungefär tre man eller färre. Och när man är tre man eller färre och försöker utveckla en ny laserdiod eller vad man nu försöker åstadkomma då tror jag många gånger att man är 100 procent fokuserad på att just göra den där laserdioden eller bygga ett filter för vattenrening eller vad det nu är. Man har sin PC och i den har man allting, det är ungefär den IT plattformen man har, och i det fallet så är ju datorsäkerhet att aldrig utsätta den PC:n man har för möjlighet till stöld… att ha ett lösenord som inte bara är enter eller fruns namn… Då har de i deras värld och ambitionsnivå uppnått ganska god datasäkerhet…

DO: Tack så hemskt mycket för tiden…

Bilaga C: Transkribering av intervju med Atea i Sverige

Intervjuare	Daniel Berntsson och Oskar Grunning
Datum för intervju	2007-05-10
Intervjulängd	30 minuter
Företagets namn	Atea
Intervjuad person	Konsult på Atea i Sverige
Intervjupersonens position	Konsult
Plats för intervju	Atea

DO är intervjuarna Daniel och Oskar *IO är intervjuobjektet hos Atea*

DO: Då är det om vi ska börja lite snabbt, börja på generell information om Atea och så där.
IO: Ja.

DO: Hur många ni är och vad ni sysslar med och så?
IO: Vi är en del av en nordisk koncern. Hur många anställda vi är i norden vet jag inte va men vi är cirka tusen anställda här i Sverige. Och vi går under namnet Atea i Sverige, Ementor i Norge, TopNordic i Danmark och Atea i Finland. Så det är de tre olika varunamnen vi kör under. Eller ja, det kan vi säga.

DO: Mmm.
IO: Och vi jobbar uteslutande med IT-infrastruktur så vi jobbar inte med någon systemutveckling.

DO: Sen var det om synen på datasäkerhet. Både här och hur ni tänker för era kunder?
IO: Ja, då skriver ni fysisk, logisk och mänsklig. Va e?..

DO: Ni har väl lite mer med fysisk, antar jag? Med strukturen, och…
IO: Ja, det gör vi ju alltså. Vi säljer ju produkter då va. Och implementerar produkter som handlar om fysisk säkerhet och logisk. Det handlar om behörighetskontrollsystem, katalogtjänster, digitala certifikat och sådana saker. Men vi jobbar också, speciellt jag då, med kunder utåt och med mänskliga, utbildning, rutiner, processer och hur man ska jobba och så vidare. Alltså, den generella synen har jag svårt att svara för. Men det är mer min generella syn på säkerheten då va. Jag tror inte vi har något sånt där riktigt, för företaget, utan det handlar om… Ja, tyngdvikten ligger snarare hos den fysiska och logiska. Om man nu ska ha en generell syn.

DO: Risker. Medvetenhet där runt om kring. Hur ni anpassar er för det ni har hittat och så där?
IO: Hur vi själva jobbar med det så, alltså vi har ju den fördelen att. När vi jobbar med säkerhet mot kunder så ser vi ju fler risker eller ja, fler händelser eller incidenter, än vad vi själva hade gjort då va. Så på det viset hämtar vi erfarenhet från våra kunder. Precis som vi delar med oss av dom till andra kunder då. Utan att avslöja var ifrån det kommer. Det är ju det det bygger på att vara konsult, att kunna dela med sig. Sen kanske det inte är riktigt… Som konsult arbetar vi nog, bättre om vad kunderna ska göra än vad vi själva ska göra. Det finns ju det uttrycket skomakarens barn går ju alltid med de sämsta skorna och det är ju lite kanske så också i de här IT sammanhangen då också va. Att vi kanske lägger krutet på våra kunder och försöker väl hinna fatt med de egna rutinerna. Men… Det gör vi ju inte alltid…

DO: Men vilken säkerhet är det som prioriteras när ni försöker implementera det för någon t.ex. en annan kund. Är det dom som väljer det eller… Av det logiska, fysiska eller mänskliga?
IO: Mmmm.

DO: Vad rekommenderar ni vanligtvis kunderna liksom för att de ska få så bra säkerhetsskydd som möjligt?
IO: Ja, jag tror vi skiftar där på vägen. Så vi är mittemellan två olika synsätt. Och det ena synsättet det är ju det att vi jobbar med produkter och implementerar det, för det är ofta det kunderna frågar oss. Men om vi sträcker oss lite längre så börjar vi, hellre då va, med en riskanalys för att få fram vilka de mesta kritiska tillgångarna de har. Och hur ser riskerna ut emot dom och… Så att kunden kan prioritera bland sina riskinvesteringar, eller riskinvesteringar… säkerhetsinvesteringar. Vilket kanske inte alltid har varit fallet innan då va. Man har lagt pengar på fel saker. Eller ja, det säger jag inte att de har va, men i och med att säkerheten har blivit så mycket viktigare så krävs det mer och mer resurser för att klara av bra informationssäkerhet. Så krävs det ju också att man prioriterar området och då är det ju bättre att började med en riskanalys för att sedan kunna… komma ner… då kanske man ser, jaa, att man behöver stärka upp den tekniska säkerheten på de nivåerna men sen kanske framförallt kanske vi behöver utbilda vår personal eller framförallt så måste ledningen diskutera säkerhetsfrågor mer ofta. Så jag tror att vi är mer på väg åt det hållet med den strategiska säkerheten istället för den taktiska.

DO: Det är lite om, du sa där i riskanalysen man väger alltså vad man prioriterar.
IO: Mm.

DO: Finns det någon risk att man prioriterar bort något, fel sak, på något sätt?
IO: Ja det är det ju.. Och jag ser en… Alltså som konsult så försöker jag och hålla mig så låg profil som möjligt i de sammanhangen. För i det fallet så tycker jag att kunden vet alltid bäst när det gäller det och kunden kan ju så himla mycket om sin verksamhet, vet systemen och så vidare. När de väl tänker efter så vet dom, bättre prioritering än om vi skulle komma och föreslå någonting. Så jag skulle säga mer riskanalysering där kunden är den som framförallt tar fram det hela va. Så gör de ett bättre investeringsbeslut än om de bara skulle ställa en fråga eller läsa en tidning eller och så vidare. Men sen självklart, de kan ju göra felaktiga bedömningar om vad som är risk och… alltså det går ju inte… det kommer alltid finnas man kan aldrig förutse alla händelser. Men om man börjar att fundera kring de viktigaste tillgångarna dom har, de mest kritiska. Då får de förhoppningsvis en möjlighet att träffa bättre då och blir då lite förberedda.

DO: Men det är mest koncentration som läggs på de stora hoten? Det är ju andra hot som till exempel spam och etiska hot som sexuell e-post och ras grejer… Det är mest på säkerhet som det läggs? Alltså i de stora… till exempel att du har en mängd data som du verkligen vill skydda, är det som krutet läggs på eller är det ett helt koncept att liksom?
IO: Dom här frågorna kring etisk… etiska frågor alltså kring surfning och vidarebefordring av mail som har med rasdiskriminering eller annan diskriminering att göra. Det är ju viktiga frågor och de brukar man ta upp i de policys då som man tar fram. Och de behöver man. För det första slår man fast det utan att lägga någon teknik på det va. Att den anställda förbinder sig om att inte surfa till sådana sidor eller att sprida sådan information. Och… Nästa steg att kontrollera att de verkligen gör den kommer nog i andra hand då va. Än de stora… Det skulle jag tro. Den är dock inte mindre viktig, alltså så. Den är ju lätt att kontrollera i och för sig. Men det är ju en annan fråga som också är etisk, eller etisk och etisk det kanske den inte är men det handlar ju om intrigitet och det är hur mycket man ska kontrollera medarbetarna med tekniken. Därför att tekniken kan ju göra väldigt mycket och då helt enkelt man är i.. ja kontrollera precis alls som medarbetarna skickar och till exempel om det är någon som jobbar på saab och skickar ett e-post med.. där det står volvo inuti meddelandet då kan det ju snappas upp av IT om de vill… Också,

jaha.. han skickar till… Eller till en volvo adress utan att den anställda får reda på det. Och det är ju också en slags oetisk, helhet i det hela. Och där får man vara väldigt försiktig då. Så det viktigare är ju att ha en utbildning kring det och att man pointerar att det inte är något vi accepterar här på den här arbetsplatsen. Om vi skulle komma på det så kan det leda till åtgärder. Som i slutet så kan det handla om att man får avsked.

DO: Det specificeras i policyn?
IO: Det specificeras i policyn, ja.

DO: Utvecklar ni, eller hjälper ni också till att utforma dom eller?
IO: Ja, då gör vi det. Vi har en diskussion med kunden så… kommer vi fram till.. äh.. ja vi har några exempelgrejor så får dom stryka och… det här är inte aktuellt hos oss, vi har ingen hemlig information om det är någon offentlig verksamhet eller någonting sånt där så då tar vi inte med det, men det där är ju bra och så filar man lite på det…

DO: Ni har en stor mall då och anpassar den?
IO: Ja

DO: Ähm, just den här säkerhetskonfigurationen eller konsultationen, efter. Uppföljs den senare, så man kollar om man har lyckats?
IO: Ja, det är iallafall meningen då va. Vi lever ju som konsulter så vi hoppas ju att vi ska få kunna komma tillbaka då, det kan vi göra då va. Men det är ju meningen att.. Det försöker vi också poängtera att det är viktigt för kunden att göra en sånhär analys varje år då, eller något sånt.

DO: Vad är det värsta som kan hända gällande datasäkerhet för kanske er själv som företag och som kund också.
IO: Det värsta som kan hända oss som företag. Jaa… *lång väntan* Allstå jag har inte varit med och gjort en sådan analys kring vårt företag så då men… Kundregistret är ju jätteviktigt.

DO: Mm
IO: Mm. Det får ju inte bara komma i händerna på en konkurrent. Men i och för sig har dom säkert… också… Alltså det som inte får hända är ju när vi gör en utredning att den… till en kund som handlar om säkerhet då och den får inte komma ut, det får den inte göra, för då tappar ju.. Då, då, tappas förtroendet för oss då va.

DO: Mm, och det är väl samma sak där egentligen då, vad som, det värsta som kan hända för en kund, blir det ju då också.
IO: Ja i det fallet är det ju det. Mm.

DO: Att den informationen skulle komma ut.
IO: Mm

DO: Arbetet för att upprätthålla säkerhetssynen. Policy, typer och områden och… Det var kanske lite där.
IO: Vi har alltså en IT-säkerhetspolicy internt, vi har också en mailpolicy kallas den väl… Nej, etiska regler för internet- och mailanvändning tror jag att den kallas. Internt. Och den utbildas alla i som anställs.

DO: Hur funkar det med lösenordshantering och sånt. Har ni en policy just för det eller det är något som ingår dom andra eller.

IO: Nej, det har vi ingen speciell policy. Utan vi bara ställer krav om att det ska vara starka lösenord.

DO: Och säkerställningen av den mänskliga riskfaktorn är det endast genom utbildning och så, eller man kan styra det på annat sätt.
IO: *lång väntan*. Ja. Genom utbildning, ja det är det ju då va. Sen lever ju vi i en väldigt konkurrensutsatt verksamhet och det är lätt att man flyttar på sig då va. Alltså blir rekryterad till ett annat företag då, konkurrerande företag och där finns det ju sådana… ah jag har vetat att det funnits klausuler men jag vet inte om de används faktiskt nu, där man har alltså kunnat sätta folk i karantän då. Att de inte har fått gått till det andra företaget förrän efter 3 månader eller något sådan där. Dom får sitta och stapla gem i källaren eller något sånt.

IO&**DO**: Skrattar…
IO: Nej jag tror inte att det är så längre. Men lite såhär är det ju, säger man upp sig.. Men det är det ju på alla företag då va. Under uppsägningstiden så får man inte jobba med någon annan verksamhet än där man är anställd alltså. Man kan ju inte liksom smyga med, och jobba men något annat under tiden som man jobbar. Då finns det ju en risk för att man blir uppsagt på direkten och inget arbetsbetyg och grejor, och så vidare.

DO: Ett vanligt företag som ni är konsulter åt, vad är den vanligaste säkerhetsutbildningen, och vad innehåller den. Vad är det ni lär ut eller vad…
IO: Det var ett tag sedan jag blev anställd bara så jag vet inte… Njae, men vi lär väl ut alltså, egentligen handlar det väldigt mycket om den här IT-säkerhetspolicyn och etik, etikreglerna då va, att… ja, var försiktig och var rättvis på något vis. Man litar till anställdas förmåga att tänka själva då va, och det är… Det är inte mycket… Det finns ju sådana här: du får inte göra det och du får inte göra det och så vidare, det finns ju sådana pekpinnar då va. Men det är rätt mycket, du ska veta att det är… att det är viktigt att uppföra sig på rätt sätt med de här grejorna vi jobbar med för att också kunna få ett förtroende hos kunderna.

DO: Lite sunt förnuft.
IO: Ja det är det, det är en hel del sunt förnuft där. Och sen är det ju, eftersom vi är tekniker så vet vi ju kanske ganska mycket mer än vad andra vet om vad som kan hända och är därmed är mer försiktiga.

DO: Ja den sista frågan har vi kommit in på också. Det är mycket kring kundens säkerhetstänkande och värderingar som tillämpas när ni utför tjänster mot dom.
IO: Ja i de fall de har en utvecklad säkerhetsfilosofi, men oftast har de inte det skulle jag vilja säga så att… Vi försöker väl… Ja en säkerhetsfilosofi kan ju i och för sig vara att man inte har någon direkt syn på säkerhet va liksom. Det är ju… Nej det kommer inte röra oss, säger dom och, nej, att folk skulle hacka oss det är ju liksom otroligt och spam lider inte vi av i alla fall. Så säger ju dom en del då va. Och… ja, i så fall får man ju påvisa då att, övertyga dom om att det kanske behövs en lite högre nivå på säkerhet än vad man själva tror sig behöva då va. Då är det ju mer våran säkerhetsfilosofi som blir påverkad. Eller så har det väldigt klart för sig vad dom vill och, ja, men då är det klart att vi också lär oss av kunderna då också då va.

DO: Det vanligaste är att när ni går in och är konsulter att dom inte tidigare har haft en ordentlig säkerhetsfilosofi.
IO: Ja, det är det nog: Det är nog vanligast. Ja.

DO: Sen är det ju den här: Har personal och ledningen delad uppfattning om säkerhet. Men det är ju med skriven mer för er som företag då om det är…

IO: Nej det kan jag inte säga att vi har någon skillnad, vi har en delad, vi delar uppfattning om man så säger.

DO: Men stöter ni på det när ni är ute någon gång att ledningen anser att det finns ett annat säkerhetsbehov än vad personalen har.
IO: Nej det tror jag inte, nej.

DO: Ja, jag vet inte om vi har så mycket att fråga. Det är väl i så fall kanske några kompletterande frågor om det skulle vara så att man kunde så svar på dom via mail eller något.
IO: Ja visst.

DO: Så hade det varit jätte jättebra. Annars tror jag inte att vi i nuläget har så mycket mer att fråga.
IO: Bara jag får ta det av uppsatsen.

DO: Ja absolut. Absolut. Vi kommer att, vi kan sammanställa denna intervjun och sen skickar vi över vad vi harkommit fram till, hur vi har tolkat detta, och så skickar vi detta till dig och sen som helhet också.
IO: Okey, men det är gött.

DO: Jättebra. Vi tackar för upptagen tid.
IO: Tack ska ni ha.

Bilaga D: Respons på intervjun med Atea i Sverige – mailkonversation

Från: "XXXX" XXXX.XXXX@atea.com den 16 maj 2007 08:09:46
Ärende: RE: C-uppsats - säkerhet - intervju
Till: Daniel.Berntsson@hermes.ics.lu.se

Hej!

Se kommentarer nedan i rött.

//XXXX

From: Daniel Berntsson [mailto:Daniel.Berntsson@hermes.ics.lu.se]
Sent: den 15 maj 2007 10:53
To: XXXX
Subject: Re: C-uppsats - säkerhet - intervju

Hej igen XXXX!

Vi har sammanställt intervjun och den text som finns nedan är den text som kommer finnas i uppsatsen som en sammanställning av intervju.

Det skulle vara uppskattat om du skulle vilja läsa igenom och kommentera om det är något vi har missuppfattat så får vi utvärdera den punkten ännu en gång, eller tillägga något som du anser att vi har missat.

Tack på förhand!

// Daniel Berntsson och Oskar Grunning

Atea är en del av en Nordisk koncern med 20-talet kontor över hela landet. I Sverige består Atea av ca 1000 anställda som tillsammans hjälper företag och organisationer genom att leverera produkter och tjänster som förenklar hantering, drift och utveckling av IT-infrastruktur såsom behörighetssystem, katalogtjänster, digitala certifikat och många fler. Företaget finns i samtliga länder i norden men går under olika företagsnamn – Ementor i Norge, TopNordic i Danmark och Atea i både Finland och Sverige.

Intervjun med Atea Sverige ägde rum på ett av deras kontor i Sverige med en erfaren konsult inom IT-säkerhet och med flertalet certifikat i bakfickan. Respondenten hos Atea Sverige arbetar uteslutande med IT-infrastruktur där kontakten mot kunden är viktig då utbildning, rutiner och processer är en del av arbetet. Respondenten svarar på frågor och ställer dem i relation till deras arbetssätt mot deras kunder då deras eget säkerhetsarbete sätts i skymundan just på grund av att de fokuserar mer på deras kunder än på sig själva. Självklart är deras egna

skydd tillräckligt då de själva har information som exempelvis kundregister och liknande som absolut inte får komma i konkurrenternas händer. De anställda på Atea Sverige är tekniskt lagda personer och detta tror respondenten kan vara en anledning till den lågt hålla säkerhetsfilosofin då de anställda vet mycket mer om säkerhet än många andra och tillämpar därmed mer sunt förnuft, men självklart finns det riktlinjer för hur man får bete sig.

skomakarens barn går ju alltid med de sämsta skorna
(konsult på Atea, personlig kommunikation, 10 maj, 2007)

Respondenten arbetar direkt med kunderna och samlar på sig erfarenheter samtidigt som han delar med sig av den kunskap som han och företaget besitter. Detta gör att han har en bred uppfattning över säkerhetsläget men anser att han inte klarat arbetet utan kundens insyn i sin egen verksamhet då de ser olika händelser och incidenter på annat sätt. I många fall har inte kunderna någon säkerhetsfilosofi applicerad på verksamheten och då försöker man övertyga eller påvisa kunden att denna behver ha en högre nivå av säkerhetstänkande. I de fall då kunden redan har en väldefinierad säkerhetsfilosofi tar konsulten erfarenhet av kundens riktlinjer. Någon skillnad mellan kundens anställda och deras lednings säkerhetsuppfattning har inte respondenten uppfattat utan anser att de båda parterna har en gemensam uppfattning. Har för mig att jag tänkte på vårt eget företag när det gällde detta. Hos kunder ser jag ofta en skillnad mellan t ex it-personalen och ledningen, där den senare inte inser vilka riskerna är.

Själva arbetet med att utveckla en säkerhetslösning för en kund börjar med en riskanalys för att få en bild över de mest kritiska tillgångarna och sedan utvärdera vilket hot dessa står inför. Kunden får sedan prioritera sina säkerhetsinvesteringar för att prioritera och satsa sina investeringar på ett annorlunda sätt än tidigare då kunden kan ha prioriterat och investerat på ett annat sätt tidigare. Det rekommenderas även att utbildning och regelbundna utvärderingar kring säkerhetsfrågorna görs med jämna mellanrum. I prioriteringsfrågorna håller konsulten en låg profil då han anser att kunden har en betydligt bättre kunskap och vet bäst hur sina egna systemfungerar om bara en eftertanke finns om hur verksamheten fungerar. Självklart finns det en risk att kunden prioriterar felaktigt men om kunden funderar på de viktigaste tillgångarna de har blir besluten kanske lite mer korrekta. De rekommenderas som Atea Sverige ger kunden angående denna typen av analys är att den bör återkomma en gång om året för att göra en uppföljning samt göra små förändringar på de punkter företaget har förändrats.

Policys finns det i begränsad mängd då man på Atea Sverige endast har policys mot etiska regler för internet- och mailanvändning och krav på att de lösenord som finns ska vara starka lösenord. Vi har en it-säkerhetspolicy också. Däremot hjälper de sina kunder med att utforma policys i samråd med kunden och med hjälp av flertalet exempelmallar som anpassas efter företagets behov. Att sedan kontrollera om de policys som finns efterföljs är en stor etikfråga. Den stora frågan är hur mycket tekniken ska få kontrollera utan att de anställdas integritet störs.

Då respondenten inte har varit med när analysen av säkerheten på Atea Sverige gjordes antog det att den värsta händelsen, ut ett datasäkerhetsperspektiv, skulle vara att kundlistan fanns tillgänglig för konkurrenterna. Denna händelse kan vara förödande både för Atea Sverige, då förtroendet minskar, men även förödande för kunden som anlitat Atea Sverige. En annan känslig punkt Atea Sverige har är att i utredningsstadiet skapas och lagras viktig och känslig information om en kund och denna information får inte heller finnas tillgänglig för utomstående.

För att säkerställa den mänskliga riskfaktorn använder de sig av utbildning men även att säkerställa att den information som de anställda ha inte kan spridas så snabbt när en person avskedas. Reglerna säger att man inte får ha två arbeten parallellt Under uppsägningstiden får man inte göra något eller läcka något till sin nya arbetsgivare men inte heller kunna byta till ett konkurrerade företag efter en viss tid efter uppsägningen. Det har funnits sådana regler förr, hur det är nu för tiden vet jag inte.

Daniel Berntsson
Systemvetenskapliga programmet
Läser INF630
Institutionen för Informatik

Bilaga E: Respons på intervjun med MOROTSmedia – mailkonversation

Från: "Filip Strandqvist" filip@morotsmedia.se den 21 maj 2007 09:51:21
Ärende: SV: C-uppsats - säkerhet - intervju
Till: Daniel.Berntsson@hermes.ics.lu.se

Det ser OK ut Daniel. Jag rekommenderar er att korrekturläsa det hela en gång till innan ni stoppar in texten i er uppsats...

Lycka till!

/Filip

Från: Daniel Berntsson [mailto:Daniel.Berntsson@hermes.ics.lu.se]
Skickat: den 18 maj 2007 16:04
Till: Filip Strandqvist
Ämne: C-uppsats - säkerhet - intervju

Hej igen Filip!

Vi har sammanställt intervjun och den text som finns nedan är den text som kommer finnas i uppsatsen som en sammanställning av intervjun.

Det skulle vara uppskattat om du skulle vilja läsa igenom och kommentera om det är något vi har missuppfattat så får vi utvärdera den punkten ännu en gång, eller tillägga något som du anser att vi har missat.

Tack på förhand!

// Daniel Berntsson och Oskar Grunning

MOROTSmedia är del av en liten koncern där MOROTSmedia, Distributed Medical och Perspektivbredband ingår. MOROTSmedia som är ett eget konsultbolag som jobbar med system- och programvaruutveckling och har 5 anställda. Filip Strandqvist arbetar som konsult och VD på företaget och har därmed även uppdrag som berör andra delar av koncernen med bland annat affärsutveckling och administrativa uppdrag.

Intervjun med MOROTSmedia ägde rum i deras lokaler i Lund i deras konferensrum som också fungerar som ett demorum för Distributed Medical. Den information som MOROTSmedia avser att skydda är känslig information, antingen för de själva eller för deras kunder. Företaget har tillgång till mängder av information hos andra företag med hjälp av olika VPN-uppkopplingar och i de fallen handlar det mycket om vilka personer som ska ha tillgång till vilken typ av information. Därför anser Filip Strandqvist att man har goda

arbetsstyrda rutiner, hanterar lösenord, in- och utloggningar på ett bra sätt. I en konsultverksamhet är det viktigt att kunna anpassa sig och leva upp till kundernas säkerhetspolicy och säkerhetsvärderingar. Filip Strandqvist anser att MOROTSmedia har en hög datasäkerhetsmedvetenhet då deras verksamhet är väldigt teknisktorienterad, men slår ett slag för ett gott helhetsbegrepp.

Att bara förlita sig på lösenord och andra liknande säkerhetslösningar är inte att rekommendera då den fysiska säkerheten är lika viktig. MOROTSmedia har bland annat pansarglas i sin lokal och har goda rutiner att stänga och låsa dörrar efter sig, även om det skulle bara bekvämt att låta dem stå öppna. Den information som MOROTSmedia lagar är oftast oväsentlig och ointressant för andra företag men väldigt viktig för MOROTSmedia. Den reella risken som finns för företaget är att någon vill ha själva utrustningen i form av datorer, tv-apparater m.m. istället för innehållet på dessa. Det västa som skulle kunna hända MOROTSmedia skulle vara om någon som har glädje av den information som de lagrar och gör ett inbrott, antingen ett nätmässigt eller fysiskt, och tar del av denna information. Ännu värre skulle det vara om den stulna informationen inte var deras. Dock blir MOROTSmedias information snabbt värdelös då de arbetar med färsk information. Intrångsservers registrerar allmänna hos som alltid förekommer såsom DDoS-attacker och diverse robotar men detta sker på en normalt låt nivå och ses inte som ett reellt hot för verksamheten. Då samtliga anställda på MOROTSmedia, enligt Filip Strandqvist, är IT-nördar så har begreppet sunt förnuft ett högre datasäkerhetsvärde jämfört men andra företag inom andra områden.

Det finns policys i verksamheten och ett kapitel i en personalhandbok handlar om IT-säkerhet och där finns riktlinjer hur man upprätthåller god datasäkerhet. Läsenordshanteringen består av krypterade och starka lösenord som roteras med jämna mellanrum. De nyanställda får även en mindre föreläsning där datasäkerhet är en av punkterna. De arbetar även med att utveckla policys åt andra företag på begäran och resultatet av detta kan vara en handbok som man senare ger utbildning i där man berättar vad som är viktigt att tänka på samt vilka konsekvenser som kan uppstå.

När MOROTSmedia utvecklar nya system från grunden arbetar de med att säkerställa en god säkerhetsmiljö bland annat genom att införa lösenordskontroller och detta kan kopplas till kundens användardatabas och på så sätt följa deras standarder. Ett annat sätt kan vara att jobba med kunder och deras nuvarande säkerhetslösningar för att sedan kunna förbättra dessa genom utbildning eller nya rutiner för att höja säkerhetsmedvetandet.

Någon skillnad mellan ledning och anställda anser inte Filip Strandqvist att det finns hos MOROTSmedia av den anledningen att de är en platt organisation då alla anställda verkar på samma nivå. I andra organisationer som man kommit i kontakt med är det alltid någon från ledningen som kommer med initiativet att göra en förändring men kan inte svara för om det finns någon skillnad mellan ledning och de anställda i andra företag.

Etiskt inkorrekta mail har finns det ingen lösning mot men i de fall man kommit i kontakt med dessa på andra företag har man löst detta genom att först se var mailet kommer ifrån sedan får dess chef ta tag i detta problem med muntlig en kommunikation. Andra kontrollerande situationer som Filip Strandqvist varit med om är i bankvärlden där man är ganska strikt och kontrollerar vilka hemsidor som de anställda besöker på arbetstid och vidtar åtgärder därefter.

integriteten är rätt så hårt skyddad i lagen i Sverige

(Filip Strandqvist, personlig kommunikation, 15 maj, 2007)

Då det är enligt lag förbjudet att läsa andras mail och avlyssna de anställda så tror Filip Strandqvist att den svenska företagskulturen är ganska okontrollerad i det avseendet.

Daniel Berntsson
Systemvetenskapliga programmet
Läser INF630
Institutionen för Informatik
