Sociala nätverk
Ett säkerhetshot bland IT-konsultföretag?

Richard Hogestadh 860127
Magnus Nilsson 810819
{gin10rho, gin10mni}@student.lu.se

LUNDS UNIVERSITET

Kandidatuppsats 15 högskolepoäng
SYSK02, Institutionen för Informatik
Framlagd maj, 2013

Handledare:
Anders Svensson

Examinatorer:
Björn Johansson
Markus Lahtinen

Sammanfattning

Titel: Sociala nätverk – Ett säkerhetshot bland IT-företag?

Författare: Richard Hogestadh, Magnus Nilsson

Utgivare: Institutionen för informatik, Lunds Universitet

Handledare: Anders Svensson

Examinatorer: Björn Johansson och Markus Lahtinen

Slutseminarium: Maj 2013

Uppsatstyp: Kandidatuppsats

Nyckelord: Sociala nätverk, risker, malware, social engineering, IT-konsultbranschen, policy

Abstrakt

Sociala nätverk är inte längre någon nyhet, men trots detta har vi funnit att medvetenheten omkring vad som delas med andra och säkerhetsmedvetandet är förhållandevis lågt. Det vi undersöker i denna studie är hur användandet av externa sociala nätverk skiljer sig bland anställda inom olika företag inom IT-konsultbranschen och hur det påverkar säkerheten inom företaget. Områden som kommer beröras är policyhantering och extern påverkan, som bland annat kopplas till om företagen upplever problem med text eller bilder som leder till skadliga webbsidor. Undersökningen kommer även beröra ämnet *social engineering* och om det upplevs som ett problem. Vi belyser ett område som det tidigare gjorts undersökningar inom, vinklat till hur ovanstående enligt väl insatta personer skiljer sig mellan olika IT-konsultföretag och vad de har gemensamt. Den litterära genomgången påvisar vilka hot som finns kopplade till internetanvändande, vilket incitament som finns för användning, och hur policy, organisationskultur, träning och utbildning kan påverka användningen och andelen direkta hot mot IT-konsultföretag.

Under våra intervjuer med fyra IT-ansvariga på IT-konsultföretag fann vi att de har ett högt säkerhetsmedvetande vilket har fått dem att använda policyer men är dåliga på uppföljning. De såg inte ovan nämnda hot som någon direkt risk för deras verksamhet. Vi kom fram till att företag som agerar inom IT-konsultbranschen inte är lika riskutsatta som företag inom andra branscher och har därför inte samma behov för säkerhetsåtgärder. Detta i jämförelse med tidigare undersökningar inom ämnet. IT-personal har också visat sig vara de som är betraktade som den grupp anställda som löper minst risk att drabbas av risker och hot.

1 Inledning

1.1 Bakgrund

Användandet av sociala nätverk på Internet ökar inom organisationer i takt med att fördelarna och möjligheterna blir fler. Det kan innebära förbättrad kollaboration inom eller mellan organisationer, bättre kundrelationer samt användas som ett marknadsföringsinstrument (Cain, 2012). I takt med att användarantalet ökar är det även möjligt att samla statistik som kan användas för produkt- och tjänsteförbättring. Samtidigt har sociala nätverk en god påverkan bland de anställda där en kombination av arbete och sociala aktiviteter ökar välmåendet (Koch, Gonzalez & Leidner, 2012). SilkRoad's (2012) studie påvisade en viss tveksamhet bland företag att låta sociala nätverk vara öppna för fri användning. De fann bland annat att 43 procent av företagen som deltog i deras studie hade en total öppenhet, 24 procent hade övervakning av användandet och 16 procent fullständigt blockerade trafik till och från sociala nätverk.

Bland de sociala nätverken finns både interna och externa varianter (se: 2.1.1) som är riktade till att användas slutet inom en verksamhet eller helt öppet där alla kan kommunicera fritt. Inom dessa två kategorier finns även tre segment som riktar in sig på olika typer av användare. Dessa kan vara privatorienterade, hybridorienterade och företagsorienterade (se: 2.1.1). Med fördelarna kring dessa sociala nätverk medförs även risker. I februari 2013 lyckades en attack att installera skadlig programvara, även kallat *malware*, på några av de anställdas datorer hos det amerikanska IT-företaget Apple (Lowensohn, 2013). Attacken antas ha använt sig av ett forum för IT-utvecklare som medel för att nå dess mål. Denna typ av attacker är en av de största riskerna för företag som använder sig av sociala nätverk enligt Ponemon Institute (2011). I studien, genomförd av Ponemon Institute som inkluderade 4 640 IT-säkerhets ansvariga, kom de fram till att anställda använder sociala nätverk oftare för icke verksamhetsrelaterade ändamål och att riskerna för *malware* ökar i takt med att användandet av sociala nätverk växer. De fann också att många organisationer inte hade tillräckliga säkerhetskontroller eller policyer för att hantera riskerna.

Sociala nätverk är något som anställda lätt kan komma åt från flera olika typer av enheter, om inga restriktioner satts upp. Det vi vet i dagsläget är att väldig många anställda har med sin egen enhet, fackspråkligt kallat "Bring your own device" (BYOD), och även kopplar upp sig på företagets nätverk. Detta medför att företagen måste säkra åtkomsten till sin data om de tänker öppna upp nätverket (Mats Karlsson, Teknisk chef WIP, Computer Sweden, februari 2013).

Ovanstående fakta ger indikationer som tyder på att organisationer har svårt att följa med i den snabba utvecklingen inom sociala nätverk. Samtidigt verkar många har en naiv inställning och vara mer fokuserade på de positiva aspekterna medan riskerna blir åsidosatta eller bortglömda.

1.2 Problemområde

Vi har valt att fokusera på externa sociala nätverk (se: 2.1.1) då dessa inkluderar omvärlden, vilket interna sociala nätverk (se: 2.1.1) inte gör. Detta innebär att vi kan förankra den problematik som påvisas ovan och undersöka om den når fram till IT-konsultverksamheter i samma utsträckning som till andra typer företag. Vi ämnar därmed undersöka vilken effekt och påverkan externa sociala nätverk har på säkerheten i IT-konsultverksamheter. Dessa verksamheter hanterar och förvaltar ofta andra verksamheters känsliga data och information, vilket gör att denna data och information kan utsättas för risker. Vi vill undersöka om dessa företag har tillräckligt hög grad av säkerhetsmedvetenhet när det kommer till riskerna relaterade till externa sociala nätverk. Vi vill även se om en eventuell policy som reglerar hur de anställda får eller förväntas agera, samt utreda hur policyn följs upp. Är dessa verksamheter i samma grad utsatta för de tänkbara hoten likt andra typer av företag, eller finns det skillnader?

1.3 Forskningsfrågor

1. På vilket sätt har externa sociala nätverken en inverkan på företag inom IT-konsultbranschen
    - Hur hög är medvetenheten beträffande säkerhetsrisker kring externa sociala nätverk inom verksamheten?
2. Har företag inom IT-konsultbranschen någon policy som inkluderar hur anställda ska agera på sociala nätverk?
    - Hur kontrolleras att policyn efterföljs?
    - På vilket sätt jobbar man för att säkerhetsnivån ska bibehållas och förbättras?
    - Räcker det att ha en policy för att minimera riskerna?

1.4 Syfte

För att övergripligt men precist undersöka vårt problemområde har vi för syfte att angripa ett antal aspekter relaterade till detta. Vi kommer därför inrama sociala nätverk per definition, undersöka vilka risker som finns relaterade till dem, se vilket synsätt verksamheter har på problemområdet, samt hur de skyddar sig både proaktivt och reaktivt. I vår studie ämnar vi även påvisa tänkbara mönsterbeteenden och tillvägagångssätt inom organisationerna. Slutligen syftar vi komma fram till riktlinjer för vad IT-konsultverksamheter bör ha i åtanke när en säkerhetspolicy, innefattande riktlinjer för brukande av sociala nätverk, tas fram. Detta för att den ska efterlevas bättre och vara enklare att följa upp. Uppsatsen är främst riktad åt personer som är ansvariga för utformning och implementering av säkerhetspolicy på IT-konsultorganisationer men kan med fördel även läsas av andra inom IT-branschen med intresse för ämnet.

1.5 Avgränsningar

Vi har valt att i första hand fokusera på säkerhetsmedvetenhet, vilka konsekvenser detta har på organisationen och vad som kan hända om risker inte uppmärksammas och tas på allvar. Därmed har vi valt bort fokus på social medvetenhet inom sociala nätverk, vilket innebär vad för information man väljer att dela, även om ämnet kort kommer att beröras för att sätta fördelarna i relation till tänkbara konsekvenser. Denna del kommer att vara begränsad till att kort belysa om det företagen uttrycker eller visar i sociala nätverk har någon positiv eller negativ effekt ur ett PR-perspektiv.

I och med detta upplägg så kommer våra frågor till respondenter och litterära återkoppling till största del vara riktad mot risker och policy för just användning kring säkerhet och inte för den sociala medvetenheten. Vidare har vi inte heller valt att fokusera på någon specifik teknisk enhet för användning, utan istället valt att undersöka hur företagen hanterar och faktiskt använder sociala medier ur ett mjukare perspektiv. Detta innebär även att vi inte kommer gå in för tekniskt i de olika hotbilderna som kan påverka organisationerna, utan mer på hur de hanterar sina anställdas beteende som kan kopplas till dessa hot och risker.

För att inte bli för breda i vår undersökning har vi valt att exkludera BYOD. Ämnet är aktuellt och nämns för att uppmärksammas men skulle i vår uppsats kunna innebära en för bred frågebas och därmed risk för att utelämna relevanta aspekter inom vårt fokusområde.

2 Litteraturbaserad genomgång

Sociala nätverk spelar en stor roll för många och har en inverkan på flera sätt. För att öka läsförståelsen vill vi därför presentera bakomliggande undersökningar och litterära kopplingar inom ämnet. Strukturen kommer börja med att bygga på en allmän skildring inom ämnet som tar dig som läsare till vårt fokusområde inom säkerhetsrisker följt av policyer som därmed kommer utredas. Vi vill börja med en genomgång av sociala nätverkens historik och användning och därmed precisera vår syn på området. Vi kommer sedan grundligt gå igenom vilka typer av hot som finns relaterade till internetanvändning och sociala nätverk, samt försöka utreda vad syftet med dessa hot är. Till slut följs allt av en kontextuell sammankoppling till organisationer gällande användning samt vilka regler och kulturella aspekter som spelar in.

2.1 De sociala nätverkens uppkomst

Uttrycket Web 2.0 myntades av Tim O'Reilly år 2003 och används ofta för att beskriva sociala nätverk. Det finns inte en fastslagen definition på vad uttrycket innebär men enligt Allen (2009) kan en förklaring vara att Web 2.0 består av de *webbsidor* som låter användare ta del av, skapa och cirkulera innehåll. Detta till skillnad från Web 1.0 där användarna enbart var konsumenter av innehåll som presenterades (Cormode, 2008). Web 2.0 har till skillnad från Web 1.0 ofta *Instant messaging* (IM) som en del av de sociala funktionerna integrerade i ett webbgränssnitt. I Web 1.0 krävs ofta att användaren laddar hem och installerade någon slags programvara för att kunna få ut liknande funktionalitet (Maness, 2006). Vidare är nästa steg i webbens utveckling Web 3.0, som närmast kan beskrivas som evolutionen av Web 1.0 och Web 2.0. Enligt Garrigos-Simon, Alcamí & Ribera (2012) kan exempelvis företag använda information som insamlats tillsammans med *data mining*, *data warehousing* och CRM (*Customer Relationship Management*) i syfte att göra produkter, märken eller tjänster mer personliga. Sociala nätverk har funnits på Internet innan Web 2.0 myntades 2003, och ett av de tidigaste är Usenet som skapades 1979 (Kaplan & Haenlein, 2010). Numera finns en mängd sociala medier som är riktade mot olika fokusgrupper. Följande fokusgrupper tas upp av Kaplan & Haenlein (2010):

Samarbetsprojekt: Har till syfte att samla flera användares simultana bidrag till ett visst projekt. Wikipedia är en typ av applikation inom denna kategori av sociala nätverk.

Bloggar: En av de första typerna av sociala nätverk där datumstämplade inlägg ofta relateras till skribentens liv i summerad form. Sköts ofta av enbart en person och för varje post är det ofta kommentarer och tankar kring det som skrivits.

Content communities: Kan vara sidor som Youtube där filmmaterial laddas upp eller Flickr där foton ladda upp. På dessa sidor behöver man inte skapa en särskild användarsida, utan det räcker med att ha en användarprofil som samlar väldigt grundläggande information.

Sociala nätverk: Vad denna uppsats kommer att ha huvudfokus på, är alltså webbsidor som möjliggör för användare att skapa användarprofiler och söka upp kontakt och socialisera med andra som också anslutit sig till nätverket. Sociala nätverk inkluderar delning och visning av det mesta, såsom text, bilder, ljud och video.

Virtuella spelvärldar: Möjliggör för spelare att framträda som personliga avatarer och interagera med andra som om det vore verklighet. Är vanligen relaterade till digitala rollspel online som exempelvis *World of Warcraft* där alla spelar möts i en artificiell värld.

Virtuella sociala världar: Är en annan grupp av virtuella världar där man skapar sin avatar och har möjlighet att interagera i en tredimensionell virtuell värld likt i verkligenheten. Här finns inga restriktioner för vad för typ av interaktion som användaren kan utföra annat än de fysiska lagarna. En variant på detta är *Second Life*.

2.1.1 Hur fungerar det och vem använder det?

Sociala nätverk har ändrat hur folk skapar nya kontakter och samspelar med varandra. En stor del av en persons sociala aktivitet kan numera ske genom ett socialt nätverk. Av de personer som regelbundet använder Internet har antalet användare av sociala medier ökat kraftigt. I en amerikansk studie av PewResearch (2013) där internetanvändares vanor undersöktes, var det genomsnittliga antalet användare av sociala nätverk 67 procent år 2012, en kraftig ökning från 2005 då det endast var 8 procent. Enligt en rapport av Nielsen (2010) där 10 länder ingick, ökade den genomsnittliga tiden som användare var aktiva på sociala nätverk med över 2 timmar per månad från 2009 till 2010, en ökning med mer än 50 procent. Enligt samma rapport är de fyra mest använda sociala nätverken Facebook, Myspace, Twitter och LinkedIn där Facebook står för mer än hälften av alla aktiva användare.

Omfattningen av de sociala nätverken har fram till idag vuxit enormt och exempelvis Facebook innehar hela 964 miljoner användare världen över (Checkfacebook, 2013). I Sverige finns strax under 4,8 miljoner användare i skrivande stund enligt Socialbakers (2013), vilket visar på en påtaglig genomströmning sett till den totala befolkningen.

Det som är gemensamt för dessa fyra webbsidor är att användare kan registrera sig, skapa, cirkulera och läsa meddelanden samt de ger möjligheten att ha ökad kontakt med andra personer. Under de senaste åren har även företag börjat utnyttja de fördelar som denna teknik erbjuder. Det finns ett flertal användarmöjligheter för organisationer som vill använda sociala nätverk (IBM, 2007). Exempelvis låter sociala nätverk användare skapa listor över personer som de tidigare arbetat, gjort affärer eller har någon annan arbetsrelation med. Eftersom listorna är kopplade till aktiva konton hålls informationen mestadels uppdaterad och underlättar framtida samarbete. Det finns även möjlighet för förbättrat kunskapsutbyte då organisationer kan använda sociala nätverk som en kunskapsbank där anställda kan lägga till och använda den gemensamma kunskapen (Van Zyl, 2008; IBM, 2007). Hur organisationer använder sociala nätverk är dock beroende av vilken typ det är.

Det finns två typer av sociala nätverk, interna och externa. Ett internt, eller stängt, är ett socialt nätverk som endast är åtkomligt för personer inom exempelvis ett specifikt företag. Det tillåter inte att obehöriga användare får tillgång till nätverket och därigenom inte heller den information som delas där. Detta ger ökad säkerhet men möjligheterna för kunskapdelning mellan organisationer eller branscher försvinner. Exempel på interna sociala nätverk är IBM's Beehive och Kaiser-Permanente's Ideabook (Koch m.fl., 2012).

Externa sociala nätverk sköts inte av organisationen utan av en tredje part och tillåter att personer utanför organisationen registrerar sig. Det kan vara privatpersoner, anställda på andra företag eller en hel organisation som en entitet. Användandet av externa sociala nätverk kan främja kunskapsdelning mellan anställda i olika företag men inom samma yrkesroll. I en studie av O'Driscoll & Cummings (2009) tolkat av Koch m.fl. (2012), använde mjukvaruutvecklare sig av Facebook och Twitter för att underlätta sitt arbete. Facebook, Twitter, Myspace och LinkedIn är alla exempel på externa sociala nätverk.

En annan typ av klassificiering som kan göras på sociala nätverk är i vilket ändamål de används för. Detta kan vara för privat- eller verksamhetsorienterat bruk, eller en kombination av de två. Nedan följer en beskrivning av de olika klassificieringarna med exempel.

Privatorienterade - Dessa sociala nätverk riktar sig endast till privatpersoner som vill interagera med andra i sitt kontaktnät. De kan vara fokuserade på en specifik typ av aktivitet eller för interaktion mellan användare. Exempel på privatorienterade sociala nätverk är MySpace som används mycket av musiker för att hålla kontakt och låta andra användare lyssna på sina låtar (Keenan & Shiri, 2009).

Hybridorienterade - Vissa sociala nätverk används både för privat bruk men kan även användas av företag för kommunikation, kunskapsdelning eller som ett marknadsföringsverktyg. Facebook och Twitter som nämns ovan kan vara populära att använda av mjukvaruutvecklare (Koch m.fl., 2012), men är för övrigt ett vanligt socialt verktyg bland privatpersoner (Keenan & Shiri, 2009).

Verksamhetsorienterade - Dessa sociala nätverk är riktade mot användande för företag eller i arbetssyfte. Bland dessa typer finns exempelvis LinkedIn, som enligt Carminati & Ferrari (2008) erbjuder användare att skapa olika typer av kontakter beroende på om det är en exempelvis studierelaterad eller arbetsrelaterad kontakt. LinkedIn möjliggör även rekommendationer mellan användare för att stärka användares anseende. En annan typ av verksamhetsorienterat socialt nätverk är Yammer som är ett internt socialt nätverk snarlikt Facebook. Det är till för att underlätta kollaborationen mellan anställda och riktar sig mot företagsanvändande (Yammer, 2013).

Som nämnt ökar antalet användare och organisationer blir alltmer medvetna om fördelarna med att ha en närvaro på och låta anställda använda sociala nätverk. Men det sker även andra ökningar i relation till detta. I Ponemon Institute's (2011) undersökning svarade över hälften av de tillfrågade IT-säkerhetsansvariga att de hade märkt en ökning i antalet

säkerhetsincidenter på grund av anställdas användande av sociala nätverk. Sociala nätverk är alltså även en attraktiv plattform att använda som språngbräda för kriminella.

2.2 Vilka är riskerna

De olika riskerna som finns på Internet är även kopplade till sociala nätverk som genom olika vis letar sig fram till slutanvändarna. Som många märkt av dyker med jämna mellanrum diverse bilder eller länkar upp på exempelvis Facebook, som ofta pekar på något extraordinärt eller annat lockande för att få så många som möjligt att välja att klicka på länken eller bilden. Vad som sedan sker är helt beroende av vad upphovsmakaren har för syfte.

2.2.1 Vanliga typer av hot

Attacker använder sig ofta av *malware* (*malicous* eller *malevolent* software) som är en övergripande term för skadlig programvara där datorvirus, trojaner, maskar och spionprogram inkluderas (Milošević, 2013). Enligt Bullguard (2013-04-02) som tillverkar skydd mot internethot kan så kallad *malware* uppdelas efter vilken typ av hot det är, där virus och maskar klassas som smittosamma hot. Därtill kommer trojaner och *rootkits* som är varianter på maskerade hot. Slutligen så finns spionprogram och *keyloggers* som är finansiella hot och designade för att stjäla information. Milošević (2013) skriver vidare att *malware* kan användas för att försämra datorers operationsförmåga, ge oauktoriserat tillträde till datorsystem eller få åtkomst till känslig information. Dessa hot är lika på många sätt men skiljer sig ofta i hur de distribueras eller vilka effekter de har. Nedan följer definitionerna för de vanligaste typerna:

Virus: Sprids genom exekverbara filer och kräver en handling av användaren för att infektera ett system. När användaren kör filen aktiveras viruset och smittar andra filer på systemet. Exakt vilka filer om smittas beror på vilket virus det är och vilket syfte det har. När systemet är infekterat kan olika saker ske, från att meddelande visas på skärmen till mer allvarliga risker, som förstörelse av lagrad data (Hughes & DeLone, 2007).

Maskar: Är autonoma hot som kan spridas utan inverkan från en användare. De replikerar sig själva bland annat genom e-mail, nätverkssystem och fildelning. När ett system är infekterat kan masken använda upp nödvändiga dator- eller nätverksresurser och därigenom minska användbarheten av systemet (Hughes & DeLone, 2007).

Trojaner: Imiterar en fil eller applikation för att få tillträde till ett system, likt den Trojanska hästen som namnet spelar på. Filen eller applikationen brukar vara något som är mycket användbart och intressant för att öka chanserna att det aktiveras. När det aktiveras är syftet att åstadkomma någon skada på det infekterade systemet, såsom att radera all data på hårddisken eller ge den som genomför attacken kontroll över det infekterade systemet (Norton; Hughes & DeLone, 2007).

Rootkit: Är mjukvara som ger åtkomst till en dator utan att administratören vet om det. Vid start tar programvaran över kontrollen av datorn innan operativsystemet kan göra det (Symantec, 2012). Vidare beskrivs att just denna typ av hot är ganska få till antalet även om det är en växande typ av problem.

Keylogger: Är en typ av *malware* som registrerar alla tangentbordsinmatningar i en loggfil och sedan vidarebefodrar informationen till exempelvis en e-mail adress (Hughes & DeLone, 2007).

Spyware: Är mjukvara som i hemlighet samlar information från det infekterade systemet och vidarebefodrar informationen via Internet. Informationen som samlas kan vara användarnamn och lösenord, bankinformation, filer eller en persons internetbeteende (Norton).

Witten & Nachenberg (2005) skriver att dessa typer av hot år 1999 låg på 281 dagars utvecklingstid från dess att säkerhetshålet upptäckts, till att det 2004 var nere på 10 dagar, vilket pekar på att intresset bland kriminella har ökat. Samma artikel beskriver att tiden för hotets spridning även förkortats och idag kan spridas till hundratusentals datorer inom loppet av ett halvt dygn. Enligt Symantec (2012) skapades det 403 miljoner nya skadliga program under 2011 vilket är en ökning med 41 procent från 2010. Symantec (2012) visade även att det bland webbsidor ansågs vara bloggar och sidor för kommunikation som innehöll mest skadlig kod.

He (2012) tar upp ISACAs (2010) fem högst graderade risker med sociala nätverk som på första plats listar virus/malware, (följt av: varumärkeskapning, bristande kontroll över innehåll, orealistiska överväntningar på internethastigheten och bristande efterlevnad för hantering av data och information). He (2012) nämner även McAfee's riskutvärdering från 2010 som påvisar att den ökande användningen av så kallade korta URL-adresser har gjort det lättare för kriminella att maskera länkar som leder till en skadlig webbsida där någon form av *malware* kan spridas. Bakom dessa länkar som kan ta användare till skadliga webbsidor så kan typen av hot variera.

Attacker kan delas upp i två varianter. Allmänna attacker försöker nå ut till en stor mängd system, medan riktade attacker är försök till att angripa specifika system eller organisationer. En vanlig variant av allmänna attacker är *drive-by*-attacker som enligt Symantec (2012) blir en allt större utmaning för både privatpersoner och företag med hundratals miljoner attackförsök varje år. Syftet med en sådan attack är således att nå ut till så många offer som möjligt (Irani, Balduzzi, Balzarotti, Kirda & Pu 2011). Symantec (2012) skriver vidare att denna typ av attack vanligen beror på att användaren klickar på en länk som tar dem till en sida som är värd för den skadliga koden. Drive-by attacker kan distribueras via e-mail men har på senare år blivit vanligt förekommande på sociala nätverk. För att stoppa eller reducera mängden skadliga länkar har Facebook implementerat ett skyddsnät som frågar användaren om han eller hon verkligen vill "gilla" en viss länk, om länken känns igen som potentiellt riskfylld (Symantec, 2012).

Den andra varianten är riktade attacker. Denna kan användas mot företag och sker i många former. Enligt samma rapport från Symantec (2012) så är det inte bara vanligt mot storföretag, utan även i hög grad vanligt mot näringsidkare med färre än 2500 anställda. Dessa företag får stå emot 50 procent av attackerna medan den högsta noteringen av attacker på 18 procent var riktade mot företag med mellan 1-250 anställda. Vidare visar undersökningen att attacker ofta är riktade mot högt uppsatta chefer, forsknings och utvecklingsavdelningar, samt personalavdelningar, där många bifogade filer tas emot, bland annat i form av Cv:n och personliga brev.

Vidare finns det, frånsett de risker och hot vi berört, naturligtvis ett antal negativa sociala aspekter som inverkar och som en organisation bör ha medvetenhet om. De sociala risker som en organisation kan utsättas för innefattar bland annat försämrat rykte, minskad effektivitet och spridning av känslig information (Field & Chelliah, 2012).

Enligt en undersökning av Economist Intelligence Unit som Aula (2010) tolkat så anser verksamhetsledare att risker gällande rykte är det största hotet mot organisationers marknadsvärde. Eftersom mycket av informationen som genereras av användare på sociala nätverk inte verifieras kan den skilja sig från en organisations uppfattning av dess värderingar. Vidare är sociala nätverk en plattform för diskussioner över hur organisationer bör agera inom känsliga frågor och en kanal för spridning av skadlig propaganda.

2.2.2 Social engineering

Ett allvarligt problem inom sociala nätverk är så kallad *social engineering* som går ut på att någon försöker få ut information och potentiella svagheter från sitt offer genom att hitta likheter och gemenskap, och därigenom uppnå sitt syfte (Workman, 2008). I en undersökning bland 853 företag baserade i England, USA, Kanada, Australien, Tyskland och Nya Zealand gjord av Dimensional Research (2011) framkom att 48 procent av alla stora företag (mer än 5000 anställda) och 32 procent av samtliga företag i studien, under de senaste två åren hade blivit utsatta för *social engineering*. Dessa attacker hade förekommit minst 25 gånger de senaste två åren och genererat ekonomisk förlust. Förlusterna grundar sig i förlorad inkomst, lägre produktivitet, samt behov av att ge IT-experter detaljerad information för att botgöra skadan. Brody, Brizzee & Cano (2012) nämner att i synnerhet banker rutinmässigt är utsatta för denna typ av försök till att bli lurade. Dimensional Researchs (2011) undersökning visade även att nyanställda och kontrakterade entreprenörer klassades som högst risk att drabbas, samtidigt som en minoritet avsåg detsamma om IT-personal.

I relation till detta har *reverse social engineering* uppstått som är besläktat med *social engineering* som namnet antyder, med skillnaden att den görs i omvänt upplägg och anses vara en ännu mer lömsk metod (Hasan, Prajapati & Vohara, 2010). Genom att använda inbyggda funktioner på ett socialt nätverk, såsom kontaktsrekommendationer, eller att uppvisa liknande intressen försöker den som utför attacken att skapa ett intresse hos offret. Nästa steg är att offret självmant tar kontakt med den som utför attacken. Eftersom offret själv skapar

kontakten finns det genast en ökad grad av tillit och därför större chans att attacken lyckas (Irani m.fl 2011).

Ett exempel på *social engineering* tas upp i en undersökning av Bakhshi, Papadaki & Furnell (2008) gjord på ett företag gällande de anställdas godtrohet i mailutskick. Där fann man att inom endast tre och en halv timme så hade 37 personer, eller 23 procent, följt en internetlänk som framstått som säker, till en webbsida innehållande en mjukvaruuppdatering som verkade komma från en betrodd källa. Bland dessa var det dock bara fyra stycken som hade klickat på knappen "fortsätt" och laddat ner mjukvaran. I studien undersöktes även företagets IT-policy där man bland annat fann dokument med direktiv gällande vad de anställda måste förhålla sig till när de använder företagets datorer. Det fanns en generell guide för användning av e-mail med bland annat riktlinjer för hur de anställda skulle handskas med oönskad e-mail innehållande bifogade filer eller länkar, men det saknades exempel material för de anställda som skulle kunna förbättra kännedomen bland riskerna. Tydlighet och lättförståelighet är med andra ord något som Bakhshi m.fl. (2008) menar är essentiellt för att användarna ska ha en rimlig chans att vara proaktiva.

2.2.3 Skydd

Förutom infektion av någon av de typer av *malware* som nämndes i kapitel 2.2.1, finns det andra konsekvenser för en organisation som blivit utsatt för en attack. I februari 2013 rapporterade Apple att de blivit utsatta för en attack via ett socialt nätverk som användes av mjukvaruutvecklare. De upptäckte att ett antal system var infekterade med *malware* som hade som syfte att sprida känslig data, något som Apple uppgav inte hade skett (Lowensohn, 2013).

Media uppger att *social engineering* ofta används för bedrägeri (Rundkvist, 2012). Även Microsoft (2013) beskriver att *social engineering* är ett sätt för kriminella att komma åt personlig information alternativt finansiell information, men även att få in skadlig kod i offrets dator. Detta styrks av Brody m.fl. (2012) som även menar att det är förhållandevis enkelt och att det faktiskt inte krävs en dedikerad hacker för att lyckas med *social engineering*.

För att skydda sig mot attacker kan organisationer använda sig av säkerhetsåtgärder i form av tekniska produkter. Dessa kan bestå av mjuk- eller hårdvara som skyddar genom att hindra åtkomst eller ta bort hot från ett attackerat system. Enligt Ponemon Institute's (2011) undersökning finns det ett flertal teknologier som föredras av IT-säkerhetsansvariga för att skydda mot attacker. Det undersökningen kom fram till var en lista med olika tekniska resurser. De mest användbara resurserna var:

Anti-malware mjukvara: Hindrar *malware* från att spridas till det skyddade systemet. Uppdateras med nya definitioner av *malware* så system skyddas i realtid. Kan även granska innehållet i komprimerade filer (Rudman, 2009).

Endpoint security solution: En helhetslösning som innefattar *anti-malware*-mjukvara, brandvägg och kontroll av data. Kan även ha datasäkerhets- och krypteringsmoduler. Finns främst för PC system men börjar även bli tillgängliga för mobila enheter (Gartner, 2012).

Secure web gateway: Agerar som filter för oönskad mjukvara eller *malware*. Innehåller även URL filter som kan användas för att blockera åtkomst till *webbsidor* och verktyg för att kontrollera aktivitet på populära applikationer. Det blir även vanligare med *secure web gateway's* som hindrar spridning av känslig information (Gartner, 2012).

Dessa tekniker är nödvändiga för att en organisation ska ha ett bra skydd mot attacker men för att ha ett heltäckande säkerhetsprogram bör även organisationen undersöka möjliga organisatoriska förändringar som kan bidra till ökad säkerhet (Rudman, 2009).

2.3 Hur ser det ut i organisationer?

Hur sociala nätverk används inom organisationer varierar brett. För vissa är det ett välkänt område medan andra är mer vilsna. Vissa företag har som tidigare omnämnt blockeringar, övervakning eller restriktioner då de anställda i och med användningen kan utsätta företaget för risker på fler än ett sätt. Detta delkapitel kommer sätta sociala nätverk bland företag i en mer kontextuell ram för att påvisa vårt fokusområde ytterligare och vad organisationer gör (eller inte gör) i proaktivt eller reaktivt syfte.

2.3.1 Användande av sociala nätverk

I dagsläget är det vanligt att många organisationer använder sociala nätverk för att stärka sitt varumärke, öka intäkter, få återkoppling och förslag på förbättringsmöjligheter (Ubeda, Gieure, de-la-Cruz & Sastre (2013). ClearShift (2007) tolkad av van Zyl (2008) framhäver att sociala nätverk ger möjlighet till förbättrade sociala kontakter, påskyndade affärsprocesser, förbättrade kundrelationer och kostnadseffektiva rekryteringar av högkvalificerad personal. Dessutom framhävs att fördelarna även innebär ökad motivation, moral och arbetstrivsel bland de anställda.

I en artikel av Huy & Shipolov (2012) undersöktes hur sociala nätverk kan användas för att skapa starkare band inom en organisation. De fokuserade på hur de fyra känslorna stolthet, glädje, hängivenhet och hur äkta organisationens användande av sociala nätverk anses vara. Enligt författarna är dessa fyra känslor stöttestenarna för det emotionella kapital anställda känner för den organisation de arbetar inom.

Äkthet: Den viktigaste av känslorna är hur äkta organisationen upplevs vara. Detta visas tydligast genom att organisationens, och dess ledares, värderingar och handlande i den fysiska världen stämmer överens med de värderingar och handlingar som sker på sociala nätverk. Om anställda ser att det finns en sann återspegling av organisationen på ett socialt nätverk kan mediet användas som en effektiv motivations- och kommunikationskanal. Detta ger större möjlighet att använda sociala nätverk för att stärka de övriga tre känslorna.

Stolthet: Befordringar och finansiell ersättning är viktigt för hur stolt en anställd känner sig över sitt arbete, men beröm och uppskattning kan också vara kraftfulla motivationsfaktorer. Med hjälp av sociala nätverk är det enkelt att visa uppskattning av en anställds arbetsprestation. Huy & Shipolov (2012) använder som exempel Tupperwares nordiska VD Stein Ove Fennes användande av Facebook för att med korta meddelande eller med Facebooks "gilla"-funktion visa beröm för försäljares prestation, något som visade sig ha stor effekt för deras motivation.

Hängivenhet: För att bygga upp anställdas hängivenhet mot organisationen är det viktigt att de känner sig del av en grupp med samma värderingar och intresse. Även om gruppens fokus inte är direkt arbetsrelaterat kan det likväl skapa en miljö som stärker kopplingar och ökar kommunikation mellan anställda. Detta leder i sin tur till diskussioner om arbetsrelaterade ämnen under och utanför arbetstid. Med sociala nätverk kan dessa grupper enkelt formas och underhållas.

Glädje: Slutligen kan sociala nätverk användas för att skapa en känsla av glädje inom organisationen. Huy & Shipolov (2012) fann att genom att använda sociala nätverk för att ha roligt med anställda kunde Stein-Ove Fenne minska klyftan mellan ledning och anställda och därigenom förbättra kommunikationsmöjligheter. I sin tur skapade detta en förhöjd känsla av trygghet och intresse hos de anställda, och ökade chanserna för innovation.

2.3.2 Organisationskultur

Enligt Dhillon (2007) är kultur inte något som kan ses eller röras utan endast tolkas genom en mängd olika diskreta eller tysta meddelanden. På så sätt kan beteende och mönster bestämda av kultur bli vidarekommunicerade i organisationen. Författaren menar vidare att det är viktigt att förmedla och tillvarata säkerhetskultur i samband med att teknologi och IT-system implementeras och används i organisationen. Problemet här kan vara att IT-system inte används som det först var tänkt och att regler relaterade till dessa IT-system och verksamhetens mål ofta är oeniga.

> *"Security culture is the totality of patterns of behavior that come together to ensure protection of information resources of a firm" (Dhillon, 2007:221)*

Dessutom poängteras bristen på ett säkerhetsmedvetande i kulturen lätt kan säkra integriteten för hela organisationen, samtidigt som det påverkar de anställdas syn och respekt gentemot IT-avdelningen. Dhillon (2007) menar att det optimala är om de anställda skulle efterfölja IS-säkerhet som om den var lika tydlig som det vardagliga livet. Detta kopplas av Dhillon (2007) till Vroom & von Solms (2004) utopiska teori om att anställda frivilligt följer alla riktlinjer. Schein (2009:21); Dhillon (2007) påvisar tre nivåer av kulturella element som kan kopplas till hur IS-säkerhet tolkas:

Nivå 1: Visuellt - låsta dörrar, lösenord, brandväggar, policyer

Nivå 2: Delvis visuellt och medvetet - strategier, kunskap om policyer, efterlevnad

Nivå 3: Ej visuellt och undermedvetet - uppfattningar, känslor, "inte göra skada"-attityd

2.3.3 Regler för sociala nätverk

För att riskerna ska minimeras behöver organisationer ha kontroll över sina anställdas användande. Detta görs på olika sätt beroende på vilken bransch och typ av företag som det gäller. Ett av sätten att öka kontroll är att stänga av all nätverkstrafik till sociala nätverk, vilket 19 procent av företag i en global studie (Clearswift 2011) gjorde, vilket var en ökning med 10 procent från föregående år. Att göra detta kan dock få negativa effekter i form av outnyttjade möjligheter. Som tidigare nämnt så kan användande av sociala nätverk inom en organisation vara mycket fördelaktigt och om tillgång till sociala nätverk stängs ner helt går organisationerna miste om dessa tänkbara fördelar. Det är heller inte säkert att det hindrar anställda från att använda sociala nätverk på arbetstid. Silkroad (2012), en organisation som bland annat utvecklar och säljer programvara för personaladministration, fann i sin studie att av de verksamheter de undersökte så använde närmare 60 procent av de anställda en mobil enhet minst en gång om dagen för att få åtkomst till sociala nätverk, och över 80 procent gjorde det minst en gång i veckan. De fann också att det inte var någon skillnad i mobilt användande på de företag som blockerade åtkomst till sociala nätverk för anställda och de som tillät. Samma studie påvisade att företagen varierade hur de tar sig an området för sociala medier. 43 procent hade fullkomlig öppenhet, 24 procent hade övervakning av anställdas aktiviteter, 16 procent blockerade allt och 14 procent var begränsade till enbart arbetsrelaterade webbsidor.

För att kunna utnyttja de fördelar som sociala nätverk erbjuder men ändå ha viss kontroll väljer andra organisationer därför att tillåta användande av sociala nätverk men inför policyer eller riktlinjer för hur de får lov att användas. Enligt Silkroad (2012) så hade 23 procent en specifik policy för användande av sociala nätverk, medan 31 procent hade en som en del av en övergripande policy. 23 procent hade ingen policy alls som heller inte berörde sociala nätverk. Ytterligare 17 procent uppgav att de hade informella riktlinjer men ingen fastslagen policy.

En policy för användande av sociala nätverk innehåller regler för hur en anställd ska uppträda vid kontakt med personer inom eller utom organisationen på ett socialt nätverk. Syftet med reglerna kan delas upp i att förbjuda, tillåta eller instruera. Exempel på regler kan vara att en anställd inte får sprida känslig information utan medgivande (Intel), tydligt ska visa att det är den anställdes åsikter som delas och inte representerar organisationen (Dell, 2011) och att stötande beteende ska undvikas (Cisco, 2012). Varken Intel, Dell eller Ciscos policyer hanterar dock hur användare ska uppträda gällande spridning av *malware* eller en attack genom *social engineering* via ett socialt nätverk.

Även om det finns en policy kan det vara svårt att kontrollera om den följs. Ponemon Institute (2011) fann att bland de IT-säkerhetsansvariga som ingick i undersökningen och arbetade på en organisation med en policy för användande av sociala nätverk, så var det hela 65 procent

som inte kontrollerade om den följdes eller inte visste om den följdes. De största anledningarna för att policyn inte upprätthölls var att det saknades styrning och översikt, att andra säkerhetsfrågor hade högre prioritet eller att det inte fanns resurser för att kontrollera att den följdes.

2.3.4 Policy - utformning och efterlevnad

En policy är tillsammans med standarder och förfaringssätt, de dokument som är del av ledningens kontrollsystem. Definitionen av en policy är en beskrivning av de handlingar som organisationen förväntar sig, eller vill hindra bland de anställda i organisationen. Olika typer av policyer kan införas beroende på vilka funktioner som ska täckas. Det kan finnas policyer för hur vissa arbetsrutiner ska genomföras, tekniska policyer som reglerar exempelvis nätverkstrafik eller vilken mjukvara som ska användas samt ledningsinriktade policyer som bestämmer vem som är ansvarig för särskilda aktiviteter. De kan vara övergripande eller ha hög detaljrikedom för särskilda funktioner. För att skapa en bra policy bör det finnas någon ansvarig och en mekanism för hur den kan efterföljas (LeVeque, 2006).

National Institute of Standards and Technology (NIST) ger exempel på en bra struktur för säkerhetspolicyer. Det går ut på att ha ett antal enskilda policyer som är fristående från varandra med en central policy som reglerar och styr hur de andra policyerna ska vara utformade. De fristående policyerna är uppdelade i problemspecifika eller systemspecifika policyer. Med denna struktur undviks omfattande policyer som täcker många funktioner, vilket har flera fördelar. Bland annat kan en omfattande policy vara svår att skriva och även svårare att implementera. Om en person i ledningen invänder mot en eller några få punkter, kan detta innebära att hela policyn inte blir implementerad. Slutligen ger NIST ett förslag på vad en policy bör innehålla. Detta inkluderar policyns syfte, omfattning, ansvarsområde och hur organisationen ska se till att den följs (LeVeque, 2006).

Som tidigare nämnt bör organisationer implementera en policy för hur anställda får använda sociala medier för att skydda sig mot de risker som kan uppstå. Det är inte bara attacker en organisation behöver vara uppmärksamma på, utan även anställdas handlande kan orsaka problem som måste hanteras. I ett uppmärksammat rättsmål i Australien fick en avskedad anställd återgå till sin gamla tjänst. Den anställde hade enligt arbetsgivaren publicerat rasistiska och sexuellt trakasserande meddelande på Facebook om två av sina chefer. En domstol fann dock att eftersom arbetsgivaren inte hade en policy för sociala nätverk så hade den anställde inte handlat på ett inkorrekt sätt, och blev därför återinsatt till sin gamla position (Fair Work Australia, 2011).

En policy för sociala medier med betoning på säkerhet är därför av stor vikt. I en litteraturgenomgång har He (2012) skrivit om vad en sådan policy typiskt kan innehålla, såsom vilken information som anställda får lov att dela med sig av, med vilken mjuk- och hårdvara sociala nätverk får användas, att anställda ska skilja på privata och arbetsrelaterade konton samt lösenordshantering. Det bör även inkluderas vilka följder som kan komma av att policyn inte efterföljs. Rudman (2009) använder Control Objectives for Information and

related Technology (Cobit), ett ramverk utvecklat för att stödja styrning av IT-tjänster, som en hjälp för utveckling av en policy för sociala nätverk. Punkter som tas upp är att en policy ska:

- Vara effektivt kommuniserbar och inte använda tekniskt jargong.
- Riktas mot en specifik målgrupp baserat på deras roller och ansvarsområde.
- Passa väl ihop med nuvarande policys.
- Uppdateras med jämna mellanrum så den är relevant
- Baseras på principer men innehålla tillräckligt med detaljrikedom för att kunna upprätthållas.

Hur man sedan framgångsrikt kan implementera en policy finns det olika teorier om, beroende på vilken slags organisation och typ av policy som ska införas. En mycket använd process är *top-down* implementation, där policyn utformas av ledningen och sedan filtreras ner genom organisationen. Detta är ofta en relativt snabb och enkel process. En negativ aspekt av top-down implementation är att fokus ligger på att kontrollera de anställdas aktiviter och möjliga konflikter kan bli ouppmärksammade. En annan typ av process är en systematisk implementering, där deltagande mellan olika aktörer är en central aspekt. För att en systematisk implementering ska lyckas behövs ett horisontellt samarbete mellan anställda och vertikal kontroll från ledningen inom organisationen (Kapsali, 2011). Även Rudman (2009) nämner att en policy ska skapas genom samarbete mellan alla intressenter och med stöd från ledningen. Författaren menar, i enlighet med LeVeque (2006), att någon inom organisationen med tillräckligt mycket auktoritet bör utses som ansvarig för att se till att policyn uppdateras och efterföljs.

2.3.5 Utbildning och träning

Även med en policy är det inte säkert att anställda följer den. I en studie som Cisco (2008) genomförde där över 2000 IT-chefer i 10 länder ingick, arbetade 34 procent av dem på företag där det fanns anställda som antingen inte visste att det fanns en säkerhetspolicy eller inte förstod den. 47 procent av dem arbetade på företag med anställda som inte ansåg att det fanns några risker med datasäkerhet att oroa sig för. Enligt He (2012) var skälet till att anställda åsidosatte policyer att de hade för dålig kunskap eller motivation samt hög tidspress för att utföra sina arbetsuppgifter.

Organisationer bör därför göra kontroller av anställdas användande av sociala nätverk. Detta kan göras genom sökningar efter särskilda sökord på sociala nätverk för att försöka hitta beteende som strider mot policyer. Enligt CDC (2009) och Clearswift (2011) tolkat av He (2012) så kan exempelvis organisationens namn användas för kontroller av felaktigt varumärkeshantering. Det är även möjligt att spara anställdas internetaktiviteter för analys.

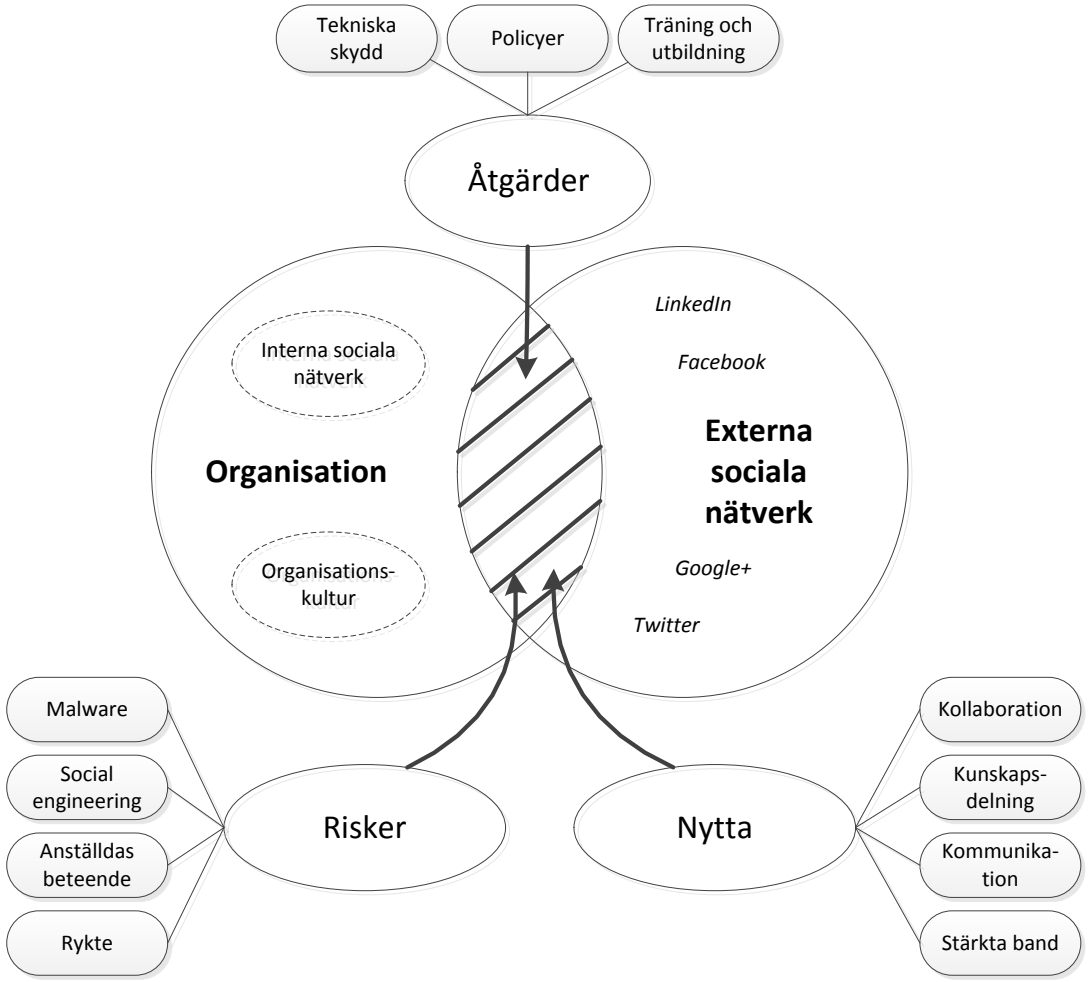
För att stärka och komplementera en implementerad policy ska regelbundna utbildningar hållas i rätt användande av sociala nätverk. Med utbildning ökar säkerhetsmedvetande för situationer där anställda kan hamna i situationer som riskerar organisationens säkerhet (He, 2012). Utbildningen behöver även hantera skillnader mellan anställdas privata och

arbetsrelaterade användande, både under och utanför arbetstid. Rudman (2009) gör i en tolkning av Cobit en punktlista över element som ska vara del av utbildning om sociala nätverk. Enligt listan ska anställda förstå vikten av datasäkerhet samt förstå och använda de säkerhetsmöjligheter som finns på sociala nätverk. De ska även kunna identifiera om en webbsida kan klassas som ett socialt nätverk, vilka risker som finns och slutligen rådfråga en IT-säkerhetsansvarig innan användande.

Dodge, Carver & Ferguson (2007) testade den amerikanska militärhögskolans elever kring risker med länkar och trovärdiga e-mail genom att skicka olika e-mail som testade studenternas förmåga att kunna undvika typiska e-mail som kan innehålla risker. Man bedömde då deras benägenhet att klicka på en inbakad länk i ett e-mail, öppna en bifogad html-fil och att följa en länk till en webbsida för att delge känslig information. Resultaten var relativt nedslående och undersökningen kunde därigenom hjälpa genom att påvisa att speciell träning behövdes inom området. Brody m.fl. (2012) åsikt kring detta är att alla företag bör använda speciella program för utbildning med jämna mellanrum för att motverka andelen lurade samt hålla tillbaka vad de kallar för autopilotbeteendet.

2.4 Sammanfattning

Sociala nätverk har en påverkan på företag på flera plan beroende på vilka val respektive organisation gjort. Riskhanteringen blir en nödvändig aspekt om organisationen inte valt att blockera åtkomsten. En ständig risk är kopplat till företagens anseende och vad som sägs om dem på sociala nätverk. Detta är i huvudsak kopplat till företag som är inriktade på försäljning till privatpersoner. Den andra sidan av riskerna är de som handlar om riktade och generella attacker i form av skadliga program och webbsidor samt *social engineering*, vilket vi valt att fokusera på i vår undersökning. För IT-konsultorganisationer är detta av extra vikt eftersom de ofta besitter känslig data tillhörande kunder. Policyer, regler, utbildning, träning och kulturella aspekter spelar en viktig roll i hur hantering och inverkan av sociala nätverk reflekteras på och i organisationen. Därför är dessa områden betydande gällande om och hur organisationer tacklar problemområdet med risker och hot relaterade till externa sociala nätverk. För att summera våra litterära fynd och därmed knyta an till vårt metodiska tillvägagångssätt har följande modell utarbetats. Modellen är en representation av den påverkan sociala nätverk har på organisationer. Den visar den nytta och risk för organisationer som kommer av användande av externa sociala nätverk samt vilka åtgärder som bör tas för att minimera riskerna.


Tekniska skydd
Policyer
Träning och utbildning
Åtgärder
Interna sociala nätverk
Organisation
Organisations-kultur
LinkedIn
Facebook
Externa sociala nätverk
Google+
Twitter
Malware
Social engineering
Anställdas beteende
Rykte
Risker
Nytta
Kollaboration
Kunskaps-delning
Kommunika-tion
Stärkta band

Figur 2.1

3 Metodiskt tillvägagångssätt

Nedan följer den process som vi genomgått för att ta fram material, underlag, samt bakgrund till de val vi har gjort under arbetsprocessen. Kapitlet kommer gå igenom de olika fundamenten med förklaringar och resonemang för våra val.

3.1 Val av metod

I och med att vårt ämnesområde har vi utgått en deduktiv undersökningsmetod. Vi vill utifrån vår litteraturgenomgång vara öppna för att se om vår tolkning av verkligheten stämmer. Därmed kommer vi använda oss av en kvalitativ undersökningsmetod, som enligt Jacobsen (2002) lämpar sig bäst för just det ändamålet. Med undersökningen vi genomförde ville vi i största möjliga mån försöka utreda hur väl företagen var insatta och förberedda mot hoten som finns tillgängliga genom sociala nätverk. Utifrån vår litteraturgenomgång skapade vi frågor som senare skulle ställas till våra respondenter, vilka var olika IT-ansvariga på de företagen vi valt ut för studien. Svaren vi fick sammanställdes till vårt analyskapitel där vi med transparens påvisar vad vi funnit under intervjuerna. Vår empiri ställdes sedan i kontrast till våra teoretiska fynd för att diskutera vilka likheter och skillnader som framkommit under de båda insamlingarna och sammanställningarna av information. Genom dessa delar hoppas vi kunna utreda huruvida IT-konsultföretag upplever sociala nätverk som en säkerhetsrisk och om deras policy infattar nödvändiga bestämmelser för de anställda. Vi vill se om våra fynd i vår litteraturgenomgång, exempelvis Cobit, stämmer överens med hur företagen i vår studie ser på problemen och hur det går tillväga.

3.2 Sekundärdata

För att skapa litteraturgenomgången har vi använt oss av olika typer av källor. Större delen bygger på information vi inhämtat från akademiska artiklar vi hittat genom artikeldatabaser. Eftersom det inte finns mycket text om vårt specifika problemområde har vi använt oss av artiklar riktade mot generell IT-säkerhet, policyutformande och implementering, *social engineering* och sociala medier. Eftersom det är ett ämne som i högsta grad är aktuellt har vi även använt oss av nyhetsartiklar som rapporterat om incidenter kring ämnet.

Data- och IT-säkerhet är en omfattande bransch där verksamma organisationer försöker vara i fronten av den tekniska utvecklingen. Det görs därför mycket forskning och undersökningar av vinstdrivande organisationer som vill hålla sig själva och sina kunder underrättade om aktuella trender. Vi har valt att använda *white papers* utgivna av bland annat Symantec, Bullguard och Silkroad. Eftersom dessa undersökningar inte granskats av en akademisk nämnd kan vi inte med säkerhet veta att de stämmer med verkligheten, men de är alla organisationer med högt anseende inom sitt område.

Forster (1994, citerad av Walliman, 2006:86) menade att:

> *"[Documents] should never be taken at face value. In other words, they must be regarded as information that is context specific and as data which must be contextualized with other forms of research. They should, therefore, only be used with caution."*

Av de vi har använt pekar innehållet åt samma slutsatser vilket stärker resonemangen. Vi har därtill använt oss av *white papers* från oberoende forskningsorganisationer som Ponemon Institute och Gartner.

3.3 Primärdata och intervjuteknik

Enligt Bryman (2001) och Jacobsen (2002) så passar kvalitativ datainsamling bra om man, som vi, har en relativt öppen forskningsfråga. Dessutom menar Jacobsen (2002) att datainsamlingen blir mer öppen för nya inslag och överraskande upplysningar. Vi har därför använt oss av kvalitativa semistrukturerade intervjuer då vi inte är så pass insatta i policyhantering gällande sociala nätverk som våra respondenter väntas vara. Ytterligare incitament för att vi valde att använda en kvalitativ ansats är att vi ämnade insamla och belysa detaljer och egenheter hos våra respondenter i den mån det gick. Vidare skriver Jacobsen (2002) att den kvalitativa datainsamlingsmetoden anses vara kostsam i mån av tid, vilket gjort att vi anpassade antalet intervjuer till fyra stycken. Med dessa intervjuer hoppades vi kunna göra en viss generalisering över hur det ser ut i IT-konsultorganisationer. Det kan anses svårt att generalisera kvalitativa undersökningar på grund av att det ofta är en liten andel respondenter jämfört med den totala summan objekt i målgruppen. För att väga upp detta krävs att empirin är detaljrik och ger en tydlig bild av ämnet. Med detaljrikedom och genom att använda läsarens sunda förnuft är det då möjligt att göra viss generalisation (Seale, 1999).

Vi har använt oss av Kvale's (1996, citerad av Bryman, 2001) kriterier för hur en lyckad intervju ska göras.

Box 15.5 **Kvale's list of qualification criteria of an interviewer (plus two others)**

Kvale (1996) has proposed a very useful list of ten criteria of a successful interviewer.

- *Knowledgeable*: is thoroughly familiar with the focus of the interview; pilot interviews of the kind used in survey interviewing can be useful here.
- *Structuring*: gives purpose for interview; rounds it off; asks whether interviewee has questions.
- *Clear*: asks simple, easy, short questions; no jargon.
- *Gentle*: lets people finish; gives them time to think; tolerates pauses.
- *Sensitive*: listens attentively to what is said and how it is said; is empathetic in dealing with the interviewee.
- *Open*: responds to what is important to interviewee and is flexible.
- *Steering*: knows what he/she wants to find out.
- *Critical*: is prepared to challenge what is said, for example, dealing with inconsistencies in interviewees' replies.
- *Remembering*: relates what is said to what has previously been said.
- *Interpreting*: clarifies and extends meanings of interviewees' statements, but without imposing meaning on them.

To Kvale's list I would add the following.

- *Balanced*: does not talk too much, which may make the interviewee passive, and does not talk too little, which may result in the interviewee feeling he or she is not talking along the right lines.
- *Ethically sensitive*: is sensitive to the ethical dimension of interviewing, ensuring the interviewee appreciates what the research is about, its purposes, and that his or her answers will be treated confidentially.

Då vi inte hade möjlighet att genomföra alla intervjuerna på plats hos kund gjorde vi även telefonintervjuer. Anledningen till detta var att många av de IT-konsultföretag vi valt att kontakta har en centralstyrd IT-säkerhetavdelning som i många fall satt stationerade i Stockholm. Telefonintervjuerna genomfördes dock med samma precision som våra besöksintervjuer, det vill säga med hjälp av inspelningar. På detta vis hade vi möjlighet att förbättra pålitligheten av de svar vi fick och på ett enkelt sätt ha möjlighet att backa bandet och se till att våra transkriberingar blev så korrekta som möjligt. Enligt Jacobsen (2002) så kan intervjuer ansikte mot ansikte tendera att ge mer känslig information, troligen då kontakten blir mer personlig än över telefon. Vi försökte dock att minimera denna faktor genom att hålla en trevlig och lättsam ton för att få respondenterna att känna sig mer bekväma. Därtill utlovades även att respondenterna skulle få möjlighet att läsa och godkänna transkriberingen för intervjun innan den betraktades som användbart material.

3.4 Intervjuguide

Fråga 1 och 2: För att positionera våra respondenter inledde vi intervjuerna med att fråga kort om befattning samt respondentens beskrivning av verksamheten. Detta breddade vår insyn och förståelse för hur verksamheten såg ut då detta gav en kompletterande beskrivning av den information vi läst på respektive hemsida.

Fråga 3, 4, 5 och 6: Vi valde att ställa öppna frågor gällande vad varje företag hade för tankar och syn på externa sociala nätverk. Vi ville här få reda på om de använde dem inom organisationen, få svar på om de haft problem som kan kopplats till användningen av sociala nätverk, och om de har någon utbildning för sina anställda. Detta härleds bland annat till stycke fyra under 2.2.1, men främst till 2.3.1 samt 2.3.5

Fråga 7 och 8: Dessa frågor ställdes relativt öppna för att få svar på hur företaget hade det med säkerhetpolicy för IT och om den innefattade delar som berörde hantering av information som inte ägs av företaget självt. Vårt antagande från start var att policyn rimligen skulle innefatta dessa delar. Detta var också för att få förståelse för om företagen rättade sig efter kundernas policyer eller om de hade sina egna bestämmelser. Dessa frågor kopplas till avsnitt 2.3.3 sista stycket samt 2.3.4 stycke tre.

Fråga 9: Med denna fråga ville vi särskilja om verksamheterna hade en policy som är specifikt riktad mot sociala nätverk, eller om den är betraktad som en mer allmän sådan. Utifrån det vi funnit i vår teoretiska referensram under 2.3.4 stycke tre, ville vi om möjligt se om verksamheterna har jobbat utifrån något särskilt ramverk då de framtagit sin säkerhetspolicy.

Fråga 10, 11, 12 och 13: Dessa frågor grundar sig i vem som är ansvarig för upprättandet och underhållet av policyn. Här ville vi även få svar på om policyn ändrats till följd av sociala mediers intåg samt om den berör flera olika aspekter och användningsområden. Vi ville även se om verksamheterna har någon form av påföljd om policyn inte efterföljs av de anställda, vilket kan härledas till punktlistan i kapitel 2.3.4 stycke fyra samt stycke fem.

Fråga 14: En fråga som vi intresserade oss för av anledningen om nyttan av sociala nätverk verkligen väger upp den mängd risker som de medför. Belyses i stora delar av vår litteraturgenomgång rörande fördelar och problem.

Fråga 15: Då uppsatsen ämnar skildra IT-konsultföretag så var denna fråga relevant för att få reda på om säkerhetshanteringen följde en viss standard utifrån det egna företaget eller om den påverkades av kundens krav.

3.5 Respondenter

När vi gjorde urvalet av respondenter var ett krav att de skulle vara väl insatta i vårt problemområde. Vi valde att rikta oss mot just IT-konsultföretag av anledning att de är mest troliga att vara potentiella arbetsgivare för oss som studerar systemvetenskap. Vi eftersträvade från start att respondenterna skulle befinna sig i Skåneregionen, men insåg att flera av företagen hade centralstyrda IT-avdelningar där kompetensen beträffande säkerhet och policy fanns. Detta medförde att vi breddade vårt geografiska urvalsområde till att företagen vi valde skulle ha kontor och vara verksamma i Skåneregionen, även om våra respondenter satt stationerade på annan plats i Sverige.

Vidare baserades urvalet av respondenter på att de ansågs vara ändamålsorienterade, innebärande att de kunde styrka den information som vi var ute efter (Jacobsen, 2002). Det främsta kriteriet för vilka vi valde att intervjua är att de besitter rätt information. Därav har vi valt att i förväg överlämna vår intervjuguide till respektive respondent för att gemensamt säkerställa att det är rätt person som besvarar våra frågor. Vi erbjöd även våra respondenter fullständig anonymitet för att de skulle känna sig säkra med att lämna ut information utan att deras anseende skulle kunna komma till skada. Detta var något som de accepterade och överlag ställde sig positiva till.

Respondent 1
R1 är IT-managementkonsult och har arbetat som konsult i 25 år inom IT-branschen. Under den tiden har titlar som IT-chef och projektledare varit aktuella och de huvudsakliga arbetsuppgifterna är projektledning av förändringsprojekt hos kunder. Mycket arbete har varit med säkerhet ur en driftsäkerhetssynpunkt, det vill säga att otillgänglighet av information och tjänster ska minimeras. Organisationen är huvudsakligen en driftsorganisation men har även outsourcing och andra IT-relaterade avdelningar.

Respondent 2
R2 arbetar på en organisation med ett antal mindre delbolag som är del av ett övergripande gruppbolag. Organisationens fokusområden är säkerhetsbranschen, automation och digital media. R2 är marknadschef och är ansvarig för gruppbolagets marknadssida utåt. Delbolagen har egna ansvarsområden men R2 har det övergripande ansvaret och har därför god insikt i alla organisationens funktioner.

Respondent 3
R3 är IT-chef på en multinationell organisation. Organisationens huvudområde är datalagringsintegration, det vill säga försäljning av datalagringsutrustning och tillkommande tjänster.

Respondent 4
R4 är IT-chef, tillika IT-ansvarig och IT-säkerhetsansvarig för en konsultorganisation med sin bas i Sverige. I sin roll arbetar han mycket inåt i organisationen för att stärka och förbättra de berörda områdena. Företaget finns i mindre skala utspridda i fyra andra länder och fokusområdena är systemutveckling och *management consulting*.

3.6 Analys av material

För att på ett pragmatiskt sätt tillgodose vår egen och läsarens förståelse för hur vi kommit fram till våra slutsatser, så har vi utifrån vårt deduktiva tillvägagångssätt gått från teoretisk bakgrund, till empiri, till diskussion. I enlighet med Jacobsen (2002) har vår analys haft fokus både på våra enskilda respondenter och situationer de relaterat till, men också till person- och situationsövergripande ämnen. Det innebär att våra respondenter både delgett oss information gällande vad de upplevt inom sin organisation och vad de har upplevt som enskild person, samt att situationer till viss mån kan vara enskilda men även jämföras mot varandra. Delar av vad vi funnit i vår litteraturgenomgång kommer ställas mot våra fynd från vår undersökning för att underbygga våra argument på ett tydligt vis. Då våra intervjuer varit explorativa kan de svar vi fått från våra respondenter skilja sig åt. Det beror i de fallen på att vi fått ett svar som lett till en följdfråga i förhoppning att få ut mer intressant information.

3.7 Etik

Vi har reflekterat över vilka etiska dilemman vi har stött på i vår undersökning. För att minimera risken att överstiga någon etisk gräns har vi handlat efter de principer som Jacobsen (2002) fastslagit.

En av principerna är informerat samtycke, alltså att respondenten är frivillig och informerad om vad undersökningen innebär. De personer vi intervjuat har vi själva tagit direktkontakt med via telefon eller e-mail. De har alltså inte fått påtryckningar från en chef eller annan auktoritetsperson att genomföra intervjun, utan haft full möjlighet att avslå vår förfrågan. Innan varje intervju har vi gått igenom vad det är vi undersöker och vad syftet är. Vi har beskrivit för respondenten hur vi kommer att använda den information vi samlar in och att undersökningen kommer att vara en offentlig handling när den accepterats. De frågor vi ställt anser vi inte vara känsliga för organisationen, förutom fråga fem som kan vara ett känsligt ämne eftersom det handlar om en potentiell negativ händelse. Hur känslig varje fråga är beror dock på respondenten och vi meddelade därför respondenterna att de inte behövde svara på de frågor de ansåg kunde skada dem eller organisationen de arbetar inom.

En annan av Jacobsens (2002) principer är krav på riktig presentation av data. Det innebär att i så stor utsträckning som möjligt redovisa resultatet av intervjun i sin helhet och i rätt kontext. För att göra detta har vi inte använt svar eller citat från intervjuerna i fel sammanhang eller förfalskat några data. Dessutom har vi transkriberat alla intervjuer och har inspelningarna tillgängliga för att styrka transkriberingarna. Vi har även skickat transkriberingarna via e-mail till respondenterna för godkännande och så de har kunnat rätta oss om vi misstolkat något av deras svar.

Slutligen så har vi meddelat respondenterna om deras möjlighet att vara anonyma, något som alla valde att vara. I praktiken innebär detta att varken de som individ eller organisationen de är anställda inom nämnts i undersökningen. All data som kan användas för identifikation av personen eller organisationen kommer därför helt att utelämnas.

4 Analys

4.1 Empiri

Med transparens kommer vi att delge vad våra respondenter gett oss för svar inom de olika områden vi har ställt frågorna beträffande. Uppdelningen av områdena är baserad på de olika frågor som vi dels tar upp i vår litteraturgenomgång, men även baserade på hur respondenterna besvarat dem. Vi frågade dels vad respondenterna hade för syn på generellt användande av externa sociala nätverk, för att även reda ut de anställdas användning av sociala nätverk och vad som var tillåtet för dem att göra. Dessa delar ville vi sedan koppla närmare hot och risker, som likt allmän internetanvändning även finns på sociala nätverk. Detta för att se om och hur företagen skyddade sig, samt vad de hade för syn på potentiella risker. Vi ämnade slutligen försöka få fram om respondenterna hade en policy beträffande våra områden samt vad den reglerade.

4.1.1 Företagens syn på sociala nätverk

Hur respondenterna ser på sociala nätverk skiljer sig mycket, från att det är ett rent PR verktyg till att det endast används för privata bruk av anställda. R4 ansåg att sociala nätverk som fenomen är relativt nytt och trodde till en början att det främst var en konsumentprodukt som används i privata sammanhang. Efterhand att sociala nätverkens popularitet ökat har R4 insett att det dels är en kanal där företag omnämns så därför bör de ha en närvaro där, men de finns där även till stor del på grund av att det anses som något man bör vara som organisation i IT-branschen. Detta sker dock med viss återhållsamhet.

> *"Vi använder inte sociala medier som en säljkanal." – R4*

Både R1 och R4 ansåg att deras kunder inte förlitar sig på sociala nätverk för att etablera och hålla kontakt med leverantörer och att sociala nätverk inte har någon riktig nytta ur marknadsföringssynpunkt. R2 och R3 ser däremot sociala nätverk som en utgångspunkt för marknadsföring.

R2 delgav även att deras organisation är mer aktiva på sociala nätverk ur en rekryteringssynpunkt, där de visar upp sin för möjliga framtida anställda på exempelvis LinkedIn. Dock skiljer sig detta beroende på vilken plattform de utgår ifrån, då de har olika syften och därmed används av organisationen på lämpligaste sätt. Där Facebook möjliggör att visa upp vad de gör för kunder så används plattformen mer som allmän kommunikation då företaget har få som följer dem där. LinkedIn är däremot platsen där de riktar sig mot tänkbar framtida arbetskraft. Även R4 ansåg att Facebook huvudsakligen är för marknadsföring men LinkedIn tillsammans med Twitter enbart är för privat bruk och var inget som tillförde organisationen direkt värde.

Både R2 och R4 var väldigt positivt inställda till Yammer, ett internt socialt nätverk riktat mot organisationer för att underlätta kommunikation och kunskapsdelning. Båda dessa

organisationer har implementerat Yammer och använder det för att snabbt dela information mellan anställda.

4.1.2 Anställdas användande

Inget av företagen har blockerat tillgång till något socialt nätverk eller är på annat vis negativt inställda till sociala nätverk. R2 ansåg istället att de var mycket positivt inställda till de anställdas privata användning av sociala nätverk.

> *"Det ser vi klart positivt på. Det är snarare den vägen vi vill gå" – R2*

De menar att de som organisation inte pumpar ut information, utan istället vill att det ska ske på individnivå. Grunden i detta är att de anser sig vara så pass stora och mångsidiga att den expertkunskap som besitts av de anställda lämpligen förmedlas av just de individer som har rätt insikt.

R2 har anställda inom organisationen som är ansvariga för hur verksamheten framställs på sociala nätverk. Dessa individer skriver och publicerar i sitt eget namn men under verksamhetens flagga. Dessa är internt utsedda till talespersoner och har förtroende att sköta hantering av verksamhetens förankring i sociala nätverk. Personerna erhåller ingen särskild träning eller utbildning och det har hittills fungerat bra att agera efter sunt förnuft. Till skillnad från detta så finns det inga utsedda talespersoner eller företagsrelaterad närvaro på sociala nätverk för organisationen R1 arbetar inom.

> *"... det [sociala nätverk] är inget som är organiserat och styrt. Det är ingen som säger vad man ska göra och inte göra" – R1*

R1 antog däremot att ett flertal anställda i organisationen är aktiva på något socialt nätverk och skriver kommentarer om företaget, men att det dock förväntas göras med respekt och förnuft. Vidare poängterades att R1 ansåg kontrollen av sociala nätverk och insikten i IT-medvetenheten överlag var väldigt låg hos kunder med både hos stora och små organisationer. Både R1 och R2 bekräftade att kraven på säkerhetshantering främst kommer på begäran av kunden.

R3 har ansvariga inom områdena marknadsföring och försäljning som arbetar utåt med sociala nätverk. Dessa är även utbildade inom området, men företaget har inte någon generell utbildning för de anställda. Därmed används sociala nätverk i det vardagliga arbetet i hur man vill nå ut till kunder och profilera sig. Skillnaden mot R4 är påtaglig i detta avseende då de mer eller mindre finns där bara för att likvärdiga företag inom samma bransch finns där.

Av de fyra respondenterna som intervjuades var det ingen som antydde att anställda använde något externt socialt nätverk som ett verktyg för kollaboration, kommunikation eller kunskapsdelning inom den egna organisationen. För detta användes enbart intern social

media, som Yammer, Lync och chatsystem. I R1:s organisation hade de försökt införa olika lösningar för kunskapsdelning men utan någon framgång.

4.1.3 Risker och hot

Få av våra respondenter såg risker och hot som ett nämnvärt problem. R4 ansåg inte att riskerna ökat i och med ökat användande av sociala medier utan att det är detsamma som vid tidigare användning av Internet. R1 uppgav att det finns risker och verksamheter måste ta ställning till om riskerna vägs upp av de fördelar som medförs. För verksamheter som levererar till ett litet antal kunder ansåg R1 att det förmodligen enbart fanns risker och att det inte fanns någon anledning att ha en närvaro på sociala nätverk. En av riskerna som R1 var mycket angelägen om var vem som ägde information om organisationen när den fanns på någon form av social media.

Trots att R2 ansåg att det fanns tydliga risker och att något snabbt kunde gå fel, var det inte värt att göra något för att minska riskerna. En policy var inte heller något som R2 ansåg skulle hjälpa i de fallen.

> *"Det enda som hjälper är ren nedstängning av access. Och kostnaden för det är så pass stor på andra håll att det inte är värt det." – R2*

Vidare ansåg R2 att eftersom organisationen innehåller säkerhetskonsulter minskar riskerna ytterligare. Enligt R2 ingår det som en del av säkerhetskonsulternas arbetsuppgifter att vara medveten om nya *malware*-hot. Om det finns risk för ett nytt hot sprider de anställda snabbt information om hotet till varandra.

Vidare uppgav även R2 att hur man ställer sig mot risker för det mesta kontrolleras genom ett avtal med kunden som styr vem som hanterar data och därmed hur den säkras mot hot och risker. R1 angav att deras nätverk som de sitter anslutna till inte är detsamma som deras gästnätverk, vilket kan jämställas med vilket stadsnät som helst. Istället sitter de i en miljö som är avskild för att säkerställa att de som är anslutna är de som har tillåtelse att vara där. På så sätt anser de sig vidtagit en viktig del av säkerhetsmedvetenheten som är nödvändig, något som R1 även framlyfte som "ren allmänhälsa". Möjligheten till att implementera mjukvara för att styra vad mobiltelefoner kan installera för appar och surfa på för sidor, vilket enligt vår respondent kommer bli vanligare inom en snar framtid.

Gällande IT-konsultverksamheter kunder så används *virtual private networks* (VPN) för att ha ökad säkerhet vid transport av data över Internet. VPN är en funktion som skapar ett avskilt nätverk mellan två system, med möjlighet att kryptera all trafik. R2 uppgav att deras VPN var ytterligare nedlåst så om någon lyckades få otillåten tillgång till nätverket så var endast viss data tillgänglig.

R1 och R4 påvisade att många kunder hade olika krav på den säkerhet de avtalade. R1 trodde att detta berodde på skillnad i kunskapsnivå hos kunderna. Kunder som hade mycket kunskap

inom säkerhetsproblem hade ofta högre och mer specifika krav som konsulterna skulle följa under uppdrag.

Ingen av våra respondenter kunde härleda eventuella problem med hot och risker direkt till anställdas användande av sociala nätverk. I stora drag ansåg tre av våra fyra respondenter att nytta vägde upp eventuella risker. R4 var den som ifrågasatte nytta:

> *"Jag ser egentligen inte nyttan med sociala nätverk på samma sätt som de flesta andra gör verkar det som. Jag ser sociala nätverk som något mer privat." – R4*

Medan R1 var positiv men avvaktande:

> *"Jag tror det beror på verksamheten[...] Alla bolag som vill synas som ser ett värde i att man profilerar varumärket måste ju vara intresserade av att delta." – R1*

Det närmaste en *social engineering*-attack någon av våra respondenter upplevt, var R3 som berättade att det för en tid sedan drevs en social kampanj mot företagets anställda. Upphovsmakarna försökte vara anonyma men relativt snart hade R3:s organisation tagit reda på vilka de var och var de jobbade baserat på den informationen de hade tillgång till. Genom informationen kunde dessa personers chefer kontaktas för att avstyra kampanjen och därigenom få det att upphöra.

4.1.4 Vad säger policyn?

Det varierade hur våra respondenter behandlade sin policy inom organisationen. Endast två av de fyra organisationer vi undersökte hade implementerat en policy som specifikt hanterade sociala medier. Av våra intervjuer framkom att R1, tillika ett av de större bolagen involverat i undersökningen, hade en väldigt uppdelad policy beroende på vilken del av företaget man satt på. På den avdelning som sysslar med outsourcing hos R1 i Malmö så finns exempelvis en anställd som ansvarar för sociala medier och säkerhet kring detta. På den avdelningen finns även ett särskilt kontrakt, ett test samt ett regelverk för området som uppdateras och kontrolleras frekvent.

Vad som generellt sätt verkar problematiskt enligt R1 och R3 är kontrollen om det efterföljs.

> *"Hur en policy efterföljs brukar alltid slå igenom av sig själv. Det är alltid någon som ser att det är någonting eller någon som inte följer policyn, så då blir det ju att man får ta upp den i varje enskilt fall." – R3*

R1 menar att det är svårt att veta om den verkligen efterföljs då de inte har någon faktisk övervakning. Detta eftersom de litar på sina anställda och därför agerar reaktivt. Dessutom finns ingen policy från koncernnivå som är kommunicerad ner till övriga delar av organisationen, men att respektive avdelning har sitt eget ansvar för detta. R3 menar att det alltid lyser igenom om en policy inte efterföljs och att de även har vissa system som håller uppsyn på hur de anställda beter sig på Internet. Däremot saknas faktiska verktyg och rutiner

för kontroll och uppföljning. R4 ansåg att de var vaksamma om organisationen fick in rapporter på att något oegentligt hade skett men hade ingen aktiv kontroll av hur anställda använde sociala medier. R1 uttryckte även att de levererar bättre kvalitet kring frågan åt sina kunder än vad de själva har.

Vidare har R3 och R4 dels en säkerhetspolicy som är övergripande, men som även hänvisar till en policy rörande just sociala nätverk och hur de anställda förväntas bete sig där. Detta är helt skiljt från R2 som tvärtom ser det som det personliga ansvar som var och en tar som konsult. De anser att de kommer upprätta riktlinjer den dagen de känner att ett behov uppstår. Det är även skiljt från R1 som uppgav att de troligen kommer att ha ett verktyg för det i framtiden. R3 uppgav även att sociala nätverkens inverkan på människor och organisationer högst troligt kommer påverka hur framtida policyer kommer se ut.

Gällande hantering av attacker genom *malware* eller *social engineering* så hade R1, R3 och R4 infört riktlinjer i deras IT-säkerhetspolicy. Åtgärderna som R4 hade var relativt grundläggande och gick ut på att ett, av ledningen godkänt, antivirusprogram skulle vara installerat på samtliga enheter, samt vem som skulle kontaktas om någon form av *malware* upptäcktes på en enhet trots antivirusskyddet. R1 hade några ytterligare specifika instruktioner för vad som skulle göras med e-mail från okända avsändare och hur anställda skulle hantera länkar eller instruktioner som skickades till dem. Dessa instruktioner var inte specifikt för sociala nätverk utan del av den generella IT-säkerhetspolicyn. R3 var ovillig att gå in på detaljer för vad policyn innehöll men nämnde att det fanns specifika åtgärder för hantering av *malware* och *social engineering*. Dessutom höll den just nu på att uppdateras och täckte in många viktiga delar. R3 nämnde även att säkerhetsseminarier och inläsning av säkerhetsinformation användes för att hålla sig uppdaterad, och på detta vis var man till 50 procent säker att informationen var aktuell.

När konsulter är ute på uppdrag hos kund uppgav R4 att det är ett krav på dem att de följer kundens policyer och riktlinjer, vilket innebär att om kunden har en särskild policy för sociala medier ska konsulterna agera efter den. R2 menar att det ofta är högre krav på konsulter än på kundens egna anställda, då konsulter kan ha extra krav gällande informationshantering och kommunikation. R1 ansåg att det var upp till kunden och att deras krav på hantering och bestämmelser bör ställas som krav.

4.2 Diskussion

I denna del jämförs de fynd som uppvisades i empirin med den litteraturbaserade teorin. Vi kommer att undersöka de skillnader som vår undersökning påvisat och om möjligt förklara varför dessa skillnader existerar. Diskussionen kommer i den mån det går att ge en generaliserad bild av hur IT-konsultföretag verkar och vilka problem de för närvarande har eller i framtiden kan stöta på. Uppdelningen av diskussionen är densamma som i kapitel 4.1 vilket ger en tydlig struktur och ökar läsbarheten.

4.2.1 Företagens syn på sociala nätverk

Företagen som ingick i vår undersökning hade överlag en öppen inställning till sociala nätverk. Två av våra fyra respondenter hade en policy särskilt riktad mot social media som den allmänna säkerhetspolicyn hänvisade till. Däri behandlades hur de anställda förväntas agera och hantera sociala nätverk mer ingående. En av våra respondenter som inte hade denna typ av policy på sin avdelning påvisade dock att det på andra avdelningar inom organisationen var betydligt mer uppstyrt. Detta kan jämföras med Silkroad's (2012) undersökning bland organisationer överlag, där mindre än vart fjärde företag hade särskilda bestämmelser för sociala nätverk. Detta kan vara ett resultat av våra respondenters branschområde där de är insatta i IT-relaterade risker och behov och därmed medvetna om vad som är nödvändigt inom organisationen.

Samtidigt har vår efterforskning fått oss att inse att personerna i dessa IT-inriktade organisationer antagligen besitter en högre snittkompetens än gemeneman gällande insikt och förståelse för hot och risker. Detta gör det enligt oss mindre riskabelt att ha en mer frisläppt policy för användningen då de anställda kan förväntas agera med bättre eftertanke, även om detta inte är garanterat. Detta faktum berörs även av Dhillon (2007) som menar att om säkerhetsmedvetenheten finns som en del i organisationskulturen så ökar integriteten för hela verksamheten. Kopplat till detta saknar vi i detta avseende uppföljning och kontroll hos våra respondenter vilket är något som vi anser vara en nödvändighet om en policy finns implementerad. Detta kan likställas med de 65 procent som inte heller gjorde detta i Ponemon Institute’s (2011) undersökning. Att samtliga respondenter saknar uppföljning kan eventuellt härledas till organisationernas tro på de anställdas förmåga att hantera användningen, vilket närmast kan kopplas till att det nästan uteslutande är IT-kunnig personal på företagen. Dock är det scenario där alla anställda följer en policy en utopisk teori enligt Vroom & von Solms (2004) tolkad av Dhillon (2007). Vi tror att det är vanligare att organisationerna blundar för det faktum att allt inte följs till punkt och pricka.

Vidare delgav två av våra fyra respondenter att de inte såg något direkt värde med att vara aktiva inom sociala nätverk. Enligt R1 och R4 så förlitar sig inte deras kunder på sociala nätverk vilket för dem gjort den marknadsföringskanalen ointressant. Tvärt emot detta så är R2 och R3 aktiva på sociala nätverk och försökte nå ut till kunder, och i R2:s fall även framtida anställda. Bland respondenterna som inte var aktiva fanns dock ingen blockering av användningen, något vi inte heller hade väntat oss med tanke på verksamhetsbransch. I och med detta tror vi att det är möjligt att tillgodose ett kunskapsbehov just denna väg. Detta faktum bekräftades även av en av våra respondenter som menade att möjligheten till användning bör baseras på nyttan. Ett större tillverkningsbolag med försäljning till agenter (företagsförsäljning) har inte någon större vinning i att tillåta användning av sociala nätverk, som R1 uttryckte. Att döma av samtliga respondenter så är inte hårda regleringar eller blockeringar något som de anser vara nödvändigt.

Bland våra respondenter så var R2 mest i framkant och i linje med van Zyl’s (2008) tolkning av ClearShift (2007) som menar att sociala nätverk stärker kundrelationerna samt ger

möjlighet till kostnadseffektiv rekrytering av högkvalificerad personal, samtidigt som de anställdas moral och trivsel ska förbättras. Dock spelar organisationens storlek och uppbyggnad in på hur sociala nätverk kan användas för att stärka kundrelationer. R2s organisation var i jämförelse till de övriga respondenterna relativt liten och även om de var uppdelade i tre mindre bolag hade de en tydlig sammanhållning. Den organisation R1 arbetade på var däremot bland de största av de vi undersökte, med mindre sammanhållning mellan de olika avdelningarna och ett stort antal fokusområden. Det är därför svårare för R1 att profilera sig på ett socialt nätverk. R1 menade att om aktiviteten på sociala nätverk visar att de ställer upp på mässor riktade till stora företag för ett specifikt fokusområde, skrämmer de bort mindre företag.

Värt att nämnas är även att internverktyget Yammer för kommunikation är något som R2 redan använder samt R4 är på väg att implementera. Detta medför enligt oss ett minskat behov av möjlighet till att använda externa sociala nätverk för intern kommunikation. Med möjligheten till att kommunicera i en sluten miljö kan tänkbart öka trygghetskänslan även bland anställda med god datorvana.

4.2.2 Anställdas användande

Enligt Clearswift (2011) var det en ökande trend med blockering av anställdas åtkomst till sociala nätverk, något som nästan en av fem verksamheter gjorde 2011. Inga av de organisationer som ingick i vår undersökning har denna typ av restriktioner för sina anställda, snarare ansåg R2 att organisationen har en positiv inställning till sociala nätverk och uppmuntrar privat bruk hos anställda. De ansåg att anställda besitter en så pass hög grad av kunskap att organisationen tjänar på att låta dem agera som talespersoner och förespråka organisationen på sociala nätverk.

Detta kan kopplas till undersökningen av Huy & Shipolov (2012) som undersökte det emotionella kapital anställda känner för sin organisation. Författarna ansåg att sociala nätverk kan användas för att öka känslan av äkthet, hängivenhet, stolthet och glädje inom en organisation genom rätt användande av sociala nätverk. Undersökningen fokuserade främst på ledningens agerande i dessa frågor men det borde även kunna tillämpas som en modell där anställda är den drivande kraften. Det som tydligast lyser igenom av detta är hur äkta organisationen upplevs vara, då skillnad mellan organisationens värderingar och anställdas kommunikation snabbt kan bli uppenbara. Hängivenhet kan byggas genom att anställda känner sig delaktiga i en grupp som delar sin kunskap med andra, och därigenom skapas en miljö med starkare kopplingar. Sociala nätverk är även en bra kanal för att ha kul och öka glädjen.

Inga av de undersökta organisationerna använde externa sociala nätverk för kunskapsdelning, kollaboration eller kommunikation mellan anställda, utan förlitade sig istället på interna system eller sociala nätverk som det ovan nämnda Yammer. Enligt R2 kunde Yammer användas både som en kommunikationskanal och som ett snabbt och effektivt verktyg för kunskapsdelning. Detta tyder på att riskerna med att använda externa sociala nätverk för att

stödja organisationers funktioner är kända och att åtgärder tas för att förbättra informationshanteringen. Med tanke på att R2 och R4 var väldigt angelägna angående Yammer's möjligheter är det troligt att denna typ av system kommer att öka i vanlighet bland organisationer med kunskapsarbetare. En del av den positiva inställningen till Yammer var enligt oss troligtvis på grund av hur likt det är Facebook, vilket gör att många användare från början vet hur man kan använda det och lite eller ingen utbildning behövs. Detta styrks även av påpekandet från R1 som menade att de äldre system de implementerat för att hantera kunskapsdelning inom organisationen inte användes.

Endast R3:s organisation har utbildning av anställda gällande sociala nätverk, och då endast för de som har som arbetsuppgift att arbeta med marknadsföring och försäljning. Ingen av de övriga respondenterna har någon form av utbildning i vad som är bra eller dåligt beteende på sociala nätverk. Enligt Cisco (2008) arbetade nästan hälften av IT-cheferna i deras undersökning på organisationer där en andel av de anställda inte var medvetna om vilka säkerhetsrisker det fanns med datoranvändning. Från informationen vi fick genom vår empiriska undersökning kan vi anta att siffran är betydligt lägre för företag som arbetar inom IT-konsultbranschen men att det är ett problem som inte försvinner helt. Detta visar att regelbundna utbildningar är av vikt för att försäkra att anställda är medvetna om säkerhetsrisker. Brody m.fl. (2012) argumenterar för detta och nämner att autopilotbeteende kan uppstå när arbetsuppgifter blir så pass välkända att arbetet blir rutinmässigt. Det är då större chans att det exempelvis sker misstag eller ett försök till en *social engineering*-attack lyckas på grund av låg uppmärksamhet. Förslagsvis tror vi att ett ramverk kan användas som grund för utbildningen, exempelvis det tidigare nämnda Cobit som Rudman (2009) undersökt. Trots behovet av träning och utbildning menar vi att anställda inom IT-konsultverksamheter kan vara i mindre behov än anställda som har datorvana men avsaknad av den expertis som är vanligare inom IT-branschen.

Ett skäl till att organisationer inte har etablerat någon utbildning och i vissa fall inte heller har en utarbetad policy för sociala medier kan vara på grund av att det är få som har haft problem. I vår undersökning hade endast R3 haft negativa erfarenheter (se: 4.2.3) gällande sociala nätverk, och i det fallet var det problem skapat av någon utanför organisationen. Respondenterna var medvetna om att det fanns risker men eftersom det inte hade haft en direkt påverkan på den organisation de arbetar inom var deras agerande av en reaktiv natur. Detta är något som stärks av ett påstående R1 gjorde, vilket var att de är reaktiva på grund av att de litar på sig själva och sina anställda. Vad R1 däremot använde sig av i proaktivt syfte var tekniska skydd som brandvägg, antivirus och övervakning, vilket samtliga respondenter hade i någon utsträckning. Dessutom fanns det inom en annan avdelning hos R1 tyngre policyer och även test för de anställda att göra för att leva upp till kraven som just den avdelningen inom organisationen ställde.

4.2.3 Risker och hot

I R2:s organisation fanns väldigt många säkerhetskonsulter och de ansåg därmed att risken för intrång eller andra hot var förhållandevis låg. Speciellt eftersom de i sina arbetsuppgifter har

specificerat att hela tiden hålla sig uppdaterade gällande de senaste säkerhetsriskerna. Detta är enligt oss ett bra incitament för att undkomma risker, då denna typ av förväntan sällan är specificerad inom mindre tekniska yrken på det sätt som R2 har det i sin verksamhet. Vi tror att det vore proaktivt om arbetsgivare hade liknande krav som åtminstone efterfrågade de anställdas förståelse för problematiken. Vi anser att det skulle vara ett steg i rätt riktning för att komma närmare den punkt där man kontrollerar att policyn efterlevs. Speciellt på ett annat sätt än R3 som trodde att det alltid på ett eller annat vis skulle komma fram om någon bröt mot policyn. Vi ställer oss frågan vilken skada som kan ha åsamkats vid det skede som det framkommer. Det behövs antagligen mer proaktivt beteende för att faktiskt kalla sig säkerhetsmedveten, vilket är ett problem som även framkommit under vår litteraturgranskning.

Risker och hot kan spridas snabbt som det framgår i vår litteraturgenomgång. Därför har både R1 och R2 som regel att snabbt sprida eventuell vetskap och information om ett problem, eller rapportera det till det till närmsta chef. Detta är något som kan ses som ett proaktivt beteende från vår sida. Att sprida den informationen internt kan snabbt och effektivt reducera risken att andra anställda drabbas. Enligt ett uttalande från R3 så fann vi att deras anställda vid ett tillfälle hade blivit utsatta för en form av anonym social kampanj, vilket var det närmsta till en *social engineering*-attack vi kunde finna. Genom uteslutning av vilken typ av information som fanns hos de som bedrev kampanjen och genom att ta reda på var de jobbade så kunde man nå fram till deras aviserare och avstyra det hela. I övrigt fann vi under vår undersökning att våra respondenter var relativt varskodda från någon form av *social engineering*-attacker. Detta stämmer ganska väl överens med undersökningen av Dimensional Research (2011) som enligt 853 IT-proffs fick fram att IT-personal var de som löpte lägst risk att bli utsatta för *social engineering*. Vi blir inte nämnvärt förvånade över resultatet i studien och kan närmast likna det vid vår egen situation. Som studerande på en IT-utbildning och med ett tekniskt intresse så anser vi oss inte att tillhöra någon hög riskgrupp, vilket kan kopplas till anställda vid IT-konsultverksamheter där förståelsen och kunskapen av oss är betraktad som högre inom området.

Samtliga respondenter har inte helt oväntat satsat på brandvägg och *anti-malware* på sina datorer. R1, R2 och R4 uppgav uttryckligen att de säkrar sina anslutningar med VPN vilket antagligen R3 också gör med tanke på deras organisationstyp. I och med att det är IT-organisationer så kan man förutsätta att de är införstådda i hur de lämpligen och på ett garanterat säkert sätt kan tillgodose de krav som ställs från kundens håll. Detta är även något som våra respondenter uttalat sig om. Ibland har kunden bra uppfattning och kommer med mer eller mindre färdiga krav på vad de förväntar sig rörande säkerheten, medan andra kunder har ett behov av att bli vägledda. Vi tror att detta gör en tydlig skillnad mellan IT-konsultbolag och generellt sett mindre tekniskt insatta bolag då förståelsen är mycket lägre i de sistnämnda. Av denna anledning pekar mycket på att risker och hot vi funnit i vår litteraturgenomgång inte förefaller sig lika naturligt i tekniskt rotade företag. Följaktligen ställer vi oss frågan om detta är något som kan bidra till någon skillnad beträffande om och hur det påverkar företagens förmåga att vara förberedda inför nya hot och risker.

Vid sidan av de tekniska riskerna finns andra risker som är av stor vikt för organisationer. Organisationen som R1 arbetade på är långt gångna med just dessa tekniska kontroller, men ett problem som R1 ansåg vara av större angelägenhet var vilken information som sprids om organisationen, och vem som äger informationen när den finns på ett socialt nätverk. Enligt Aula (2010) var just risker för försämrat rykte ett av de största hoten mot organisationers marknadsvärde. Det är därför viktigt att det finns kontroll av den information som sprids via sociala nätverk eftersom informationen snabbt kan nå stora mängder användare. Ett sätt att öka kontrollen är att göra regelbundna sökningar på sociala nätverk efter specifika sökord. I He's (2012) tolkning av CDC (2009) och Clearswift (2011) uppges att exempelvis organisationens namn kan användas för att hitta instanser där varumärke används felaktigt. För stora organisationer ger en sådan sökning förmodligen ett stort antal sökresultat vilket kan vara resurskrävande att undersöka. Istället kan fler sökord användas för att filtrera sökningen och ge tydligare resultat. Det bör även finnas människor vars arbetsuppgifter till del går ut på att övervaka och interagera med användare på sociala nätverk.

4.2.4 Vad säger policyn?

Det vi fann under vår undersökning var att uppföljningen för att kontrollera om regler och policy efterföljs var knapphändig. Mycket av ansvaret ligger på var och en av de anställda själva där de både ska hålla sig införstådda och uppdaterade beträffande företagets policy. Detta är en motpol till Rudman (2009) som poängterade vikten av att någon med viss auktoritet inom företaget faktiskt uppdaterar och kontrollerar att policyn efterföljs. Vår uppfattning från våra respondenter är att de är medvetna men trots det ser ganska lugnt på problemområdet.

R3 uppgav att de just nu håller på och uppdaterar sin policy och att den täcker in väldigt mycket. R3 var också rätt säker på att sociala nätverkens utveckling kommer att påverka policyn då det är ett levande dokument som måste följa med i tiden. Samtidigt så menar R3 att policyer och riktlinjer endast kan styra till viss del, men att man måste ta hänsyn till människors beteende. Detta kan härledas till en av ramverket Cobit's ståndpunkter som Rudman (2009) refererar till, där en policy bör baseras på principer men innehålla tillräckligt med detaljrikedom för att kunna upprätthållas. Vår tolkning av detta är att det som står i policyn måste vara tydligt och enkelt nog för de anställda att förstå, samtligt som den bör kännas naturlig att efterfölja. Frågan är dock om en säkerhetspolicy som kopplas till ytterligare en policy för sociala nätverk är ett tillräckligt enkelt sätt att distribuera ut verksamhetens regler och motiveringar till vad som är tillåtet för de anställda att göra på sociala nätverk. Enligt Cobit's rekommendationer så ska detta fungera så länge den passar väl ihop med de policyer som redan finns. Detta är något som även NIST förespråkar och menar är lättare att implementera och efterleva (LeVeque, 2006). Vi tolkar detta som att en policy med för stor omfattning ger sämre effekt än en grundpolicy som är kopplad till olika områden som subpolicyer. Detta stämmer även överens med hur R3 och R4 har byggt upp sina policyer.

En policy ska enligt Rudman's (2009) tolkning av Cobit riktas mot en specifik målgrupp baserat på deras roller och ansvarsområde. Vi tror att många företag har en generell policy som riktas mot flera olika delar i företaget, men att det kan bero mycket på hur stor verksamhet det rör sig om. Detta styrks av att det visade sig att R1 som är en del av en väldigt stor verksamhet, har olika policyer beroende på var i organisationen som man befinner sig. Dock så påpekade R1 att det var relativt lössläppt beträffande policyer inom företaget och varje avdelning själv ansvarar för den, och någon centralstyrd policy från koncernen var inte kommunicerad. Fördelen med detta är att varje policy kan anpassas efter varje målgrupp och att kontrollen av den kan bli enklare. Samtidigt finns det enligt oss en risk i att ledningen inte har insikt i det som råder och som kan tänkas vara nödvändig. På detta sätt blir det dessutom väldigt många personer som är involverade i att ta fram och följa upp nödvändiga bestämmelser för just sitt kontor eller avdelning, vilket vi tror kan splittra företaget sett till en säkerhetssynvinkel. Samtidigt kan det även bidra till möjlighet till kontroll att policyn efterlevs då det blir mindre ansvarsgrupper för de som har fattat beslut om hur policyn ska se ut.

Med en del i vår undersökning ville vi få reda på hur företag skyddar sig mot attacker med hjälp av policyer. R1 hade som en del av deras IT-säkerhetspolicy att anställda inte skulle öppna e-mail från okända avsändare och hur de skulle hantera länkar och instruktioner som skickades till dem. Även R3 hade direktiv för hantering av *malware* och *social engineering* men ville inte gå in på detaljer om vilka dessa åtgärder var. Även om åtgärderna som nämns är generella visar de att ett säkerhetsmedvetande förespråkas vilket kan liknas vid undersökningen som Bakhshi m.fl. (2008) genomförde. Deras studie påvisade att 23 procent av de anställda som öppnade en fejkad avsändares e-mailutskick innehållande en länk för nedladdning, kan minskas med de hänvisningar som R1 har i sina policydokument. Där finns det allmänna förhållningssätt som talar emot just detta. Hur pass väl de efterföljs är svårare att säga då direkt uppföljning saknas, även om det möjligen skulle märkas om en dator på något sätt var infekterad.

Vi anser att det i detta fall kan vara tillräckligt med att beröra hantering av e-mail och bilagor i policyn för att anställda i IT-företag ska ha förståelse för att veta hur de ska agera. Detta i enlighet med Dimensional Research (2011) undersökning som påvisade att IT-personal löpte lägre risk att drabbas av sociala attacker. Vi tror däremot inte att det stämmer lika väl in på en organisation som inte besitter samma tekniska kunskap som våra respondentföretag gör. I företag som inte är i IT-branschen väger antagligen någon form av utbildning vid sidan av förståelse av policyn tyngre. Exempelvis kan policyn beskriva vad som gäller beträffande systemuppdateringar och att dessa ska skötas av företagets IT-avdelning. Har en anställd övergripande koll på företagets policy men saknar utbildning finns det en risk att ett tillsynes pålitligt e-mail öppnas och får användaren att installera en uppdatering som i själva verket är skadlig programvara.

Avslutningsvis är vårt intryck att våra respondenter nog hade en mer lättsam syn på problemområdet är vad vi först hade förväntat oss. Vi var medvetna om att den tekniska kompetensen var betraktad som högre än på mindre teknisk inriktade verksamheter. Men till

skillnad från vår egen situation så är det trots allt företaget som får utstå konsekvenserna som kan medföra en kostnad, vilket Dimensional Research's (2011) undersökning visade. Vi trodde även att IT-företagen vi pratade med skulle vara längre fram gällande utbildning bland de anställda trots att vi ställde oss något ifrågasättande till hur högt behovet faktiskt var. Följande insikter har lett oss fram till en rad slutsatser som presenteras i kommande kapitel.

5 Slutsats

5.1 Resultat

- På vilket sätt har externa sociala nätverk en inverkan på företag inom IT-konsultbranschen
    - Hur hög är medvetenheten beträffande säkerhetsrisker kring externa sociala nätverk inom verksamheten?

Genom vår undersökning har vi kommit fram till att IT-konsultorganisationer inte använder externa sociala nätverk i någon större utsträckning för olika typer av arbetsrelaterat samarbete mellan anställda. Istället används det i varierad utsträckning som ett marknadsförings- och rekryteringsverktyg. Förutom detta användes även externa sociala nätverk för privat bruk av anställda, något som alla organisationer i undersökningen var medvetna om. I ett fall uppmuntrades till och med anställda att använda sociala nätverk privat och därigenom agera som talespersoner för organisationen. Istället för att använda externa sociala nätverk valde vissa organisationer istället att implementera ett internt socialt nätverk. I båda fallen var det Yammer som de båda valt att satsa på, där den Facebook-liknande strukturen antagligen bidrar till enkelheten kring användningen. Vi tror att denna typ av system kommer att öka i popularitet framöver eftersom det använder ett beprövat format som fungerar bra för snabb kommunikation och kunskapsdelning

Enligt vår undersökning visade sig IT-konsultverksamheter ha ett högt säkerhetsmedvetande gällande ämnet ifråga, något som stämmer överens med det vi fann i vår litteraturgenomgång, där IT-personal betraktades som de som löpte lägst risk att drabbas. De litar även till stor del på sina anställda, vilket vi kommit fram till stor del kan bero på att de anställda har en god teknisk kompetens. I hälften av våra respondenters fall jobbar de med just säkerhetshantering, vilket kan tänkas utöka denna kompetens ytterligare. Utbildning och träning kan vara nödvändigt, men i lägre utsträckning när det kommer till IT-konsultverksamheter. Dock kan det enligt oss finnas en risk med detta, vilket vi tror kan bero på att verksamheterna är naiva och invaggade i tron att de är i högre säkerhet än vad de faktiskt är. Detta kan visa sig i att enbart det reaktiva beteende som några av organisationerna påvisat, i framtiden slår tillbaka mot dem. Vi fann även att det fanns god medvetenhet gällande riskerna för *social engineering* och *malware* via externa sociala nätverk. Men trots detta och de tekniska skydd som IT-konsultverksamheter har, försvinner inte hotbilden fullständigt. Vår slutsats här är dock att IT-konsultverksamheter i lägre grad är utsatta för risker tack vare den kunskap som finns inom organisationen.

- Har företag inom IT-konsultbranschen någon policy som inkluderar hur anställda ska agera på externa sociala nätverk?
    - Hur kontrolleras att policyn efterföljs?
    - På vilket sätt jobbar man för att säkerhetsnivån ska bibehållas och förbättras?
    - Räcker det att ha en policy för att minimera riskerna?

Av de organisationer vi undersökte hade hälften en specifik policy som hanterade anställdas användande av sociala nätverk, med ytterligare en respondent som trodde att en policy skulle bli aktuell när organisationens omstruktureringar var genomförda. Det fanns ingen tydlig koppling mellan organisationernas storlek eller struktur och vilka företag som hade, eller inte hade, en policy för sociala nätverk. Dock hade samtliga en generell IT-säkerhetspolicy som hanterade skydd mot *malware* och i ett fall även hur anställda skulle handla om länkar eller instruktioner skickades till dem från en okänd avsändare. Gällande policy för sociala nätverk fanns det inte i något fall någon kontroll för hur policyn efterföljdes. Organisationerna uppvisade istället ett reaktivt beteende och väntade på att en incident skulle inträffa innan man vidtog någon åtgärd. Även gällande utbildning agerade de på ett liknande sätt, och valde att inte ha någon utbildning för nyanställda utan förlitade sig på att anställda höll sig själva uppdaterade om nya säkerhetshot. Skälet till att det inte fanns någon kontroll eller utbildning är den höga tillit som organisationerna hade till anställda i kombination med att de inte upplevt några negativa incidenter. Dessa fynd kan tänkbart kopplas till Dhillon's (2007) teori där de kulturella säkerhetsaspekterna utgör beteenden inom en organisation och tillsammans bidrar till ett viktigt skydd för informationen i verksamheten.

För att våra respondenter ska kunna vara säkra på att de inte utsätts för risker och hot, visade det sig att de till största del förlitar sig på att det som står i policyn och de tekniska hjälpmedel de installerat. De verkade till stor del nöjda med att eventuella övertramp skulle påvisa sig per automatik och att de anställda förhoppningsvis skulle bete sig som organisationen efterfrågat. Eftersom det fanns ett stort tillit till anställda i de undersökta organisationerna, fann vi även att det var tillräckligt att ha en policy för att göra företagen pålästa. Vi menar dock att policyerna i sig inte är grunden för de anställdas säkerhetsmedvetande även om de tillför ett kunskapsvärde för verksamheten gällande hur de anställda förväntas agera. Att uppdatera policyn är nödvändigt för att bibehålla säkerhetsnivån, men inte ett speciellt aktivt arbetssätt för att förbättra den.

5.2 Förslag till vidare forskning

Vi har valt att inte göra en djupare undersökning av de tekniska plattformar som kan användas för åtkomst till sociala nätverk, men känner att detta är något som hade varit intressant för vidare forskning. Framförallt att titta på effekterna av mobila enheter och den allt vanligare trenden att anställda använder sin privatägda mobila enhet för att komma åt verksamhetsspecifik information, även kallad *bring your own device* (BYOD). På grund av de nya problem som uppstår när flera olika typer av mobila enheter ska beviljas säker åtkomst till organisationers nätverk, tror vi att det kommer att kräva en förändring i strukturen på

nätverkens uppbyggnad och säkerhetslösningar. Detta kommer i sin tur innebära krav på en uppdatering av organisationers policy för användning av sociala nätverk (Gatewood, 2012).

Ett annat intressant ämne är effekterna och säkerhetsproblemen med interna sociala nätverk. I vår undersökning har vi valt att främst utforska externa sociala nätverk, och vad vi funnit var att en del organisationer har, eller är i färd med att, implementera det interna sociala nätverket Yammer, som stöd för organisationens funktioner. Yammer är till uppbyggnad mycket likt välkända externa sociala nätverk men många av säkerhetsriskerna är inte närvarande eftersom det är strukturerat så användare endast kan kommunicera med personer med samma typ av e-mailadress och därför ofta inom samma organisation. Tack vare dess likhet med Facebook i utseende och användning krävs det lite eller ingen utbildning och det kan snabbt användas för olika typer av stödjande funktioner. Det som hade varit intressant för vidare undersökning är vilka säkerhetsproblem som uppstår och som organisationer bör ha i åtanke vid implementation av interna sociala nätverk. Mailadress

Bilagor

Intervjuguide

1. Vilken befattning har du?
2. Hur skulle du kort beskriva verksamheten?
3. Vad har organisationen för syn på sociala nätverk?
4. Används sociala nätverk som del av det dagliga arbetet inom organisationen?
5. Har det någonsin uppstått problem p.g.a. anställdas användande av sociala medier?
6. Har ni utbildning/träning för anställda gällande sociala medier?
7. Hur säkerställer ni hantering av andra företags data och information?
8. Hur ser er säkerhetspolicy för IT ut?
9. Har ni en del i policyn för sociala medier eller är den allmän?
    a. Om "ja": Hur skapades den? (Ramverk, ex. Cobit, av ledning, överenskommelse bland anställda?)
    b. Om "nej": Hur funkar det då? Hur kommunicerar ni ut vad som gäller i avseendet?
10. Vem inom organisationen ansvarar för uppdatering och implementering av policyn?
11. Har säkerhetspolicyn ändrats/påverkats sedan sociala nätverk blev alltmer populärt?
12. Innehåller er säkerhetspolicy speciella riktlinjer för hur de anställda får använda sociala nätverk?
    a. Med egen enhet på företagets nätverk (BYOD)?
    b. På företagets datorer?
    c. På företagets mobila enheter?
    d. Riktlinjer för vad som bör göras vid hot av exempelvis malware eller social engineering?
13. Hur kontrollerar ni att policyn efterföljs?
14. Väger nyttan med sociala nätverk upp riskerna?
15. Märker ni eller gör ni någon skillnad på olika kunder beträffande säkerhetshanteringen?
    a. Ställer kunder olika krav?
    b. Får ni rätta er efter kundernas policy med sociala nätverk och säkerhetshantering och påverkas det av om konsulten sitter hos kund eller ej?

Transkribering R1

RH: Vilken befattning är det du har?

R1: Jag är konsult. IT management står det på mitt visitkort. Jag jobbar med IT styrning, så det är administrativa frågor jag arbetar med. Projekt inom IT-säkerhet, informationshantering. Vad jag gör i praktiken är det man skulle kunna kalla projektledning, förändringsarbete hos kunder och övervaka och driva på frågor. Det är min bakgrund, jag har jobbat väldigt mycket med IT-styrning. Jag har varit IT-chef 3-4 år på något bolag. Även med (…) koncernen, (…), (…) så har jag jobbat i dialog med deras group-IT inom vissa områden. Vi har varit referensgrupp när de drivit på förändringsarbete, ex föra in VPN lösningar. De vill göra förarbete, göra testningar, dokumentera och driftsätta. Då har vi varit med men när det går i drift så tar de över ansvar själva.

MN: Så ditt arbete är mest riktat åt säkerhet?

R1: Jag har jobbat 25 år i branschen. De första 5-6 åren var det mer traditionellt, då var jag projektledare och jobbade mycket med tekniker. Jag var konsultchef och satt med kunder när de tog in ny teknik. Detta var på nittiotalet, när internet gjorde sitt intrång. Då skulle man sätta upp brandväggar, mail och DNS: er. Sen när kunderna tog över driften själva så blev det lite mer frågor kring extern access och webbfunktioner, allting var ju nytt på den tiden. Jag gjorde allting som hade med bakgrundsarbete och satt i dialoger med chefer. Där det slutade var, Hur kan vi vara säkra på att det här fungerar? Så säkerhet, ja. Men det var inte så att jag satt med krypteringslösningar eller att det skulle vara hemligt, utan det var att säkerställa att det fungerade. Vad har vi att jobba med, hur vet vi att det gör det vi vill och så vidare. Det kan du sätta som rubrik på vilket projekt du vill, det är exakt samma fyra komponenter, oavsett om det står säkerhet, marknadsföring eller ekonomi ovanför. Jag har suttit på (…) och gjort sårbarhetstester och satt upp policy-ramverk. Man sätter upp någonting och sen vill man kontrollera, funkar det eller inte. Det är säkerhet i någon mening. Det var ju som när virusuppbrotten kom vid 2000, Linda och så, de får stor inverkan på bolag som (…) med 14000 enheter. Då finns det något att göra, samma som när SOX lagstiftningen kom. När företag som är USA ägda eller har kontor i USA drabbas av nya lagar eller förordningar måste de göra en massa saker. Det var ju en drivkraft i sig, för tio år sedan. Idag är man lite mer fokuserad på varför gör vi saker och vilken förtjänst får vi av det?

RH: Kan du kort beskriva bolaget (…), du nämnde outsourcing bland annat?

R1: Bolaget (…) är i omstrukturering. (…) bildades för ett år sedan, ganska precis. Det är tre stora företag, (…), (…) och (…). De tre har varit ett bolag rent ägarmässigt i flera år men det var inte förrän ett år sedan som de enades under det nya koncernnamnet (…). De här tre bolagen är väldigt olika i sin grundstruktur, (…) är norskägt, 6000 anställda, konsultverksamhet och toppstyrt. (…) som var 1200-1500 anställda är ett småländskt bolag. Man kan säga att det är 65 bolag med 20 anställda. Det är monumentalt olika sätt att driva en verksamhet på. Och den här delen som jag sitter på här, vi har varit två olika företag. Den stora enheten, det som jag kallar outsourcing är 80-100 anställda, de hette (…) tidigare. Vi på andra sidan dörren, där sitter åtta olika juridiska enheter. Vi har mobiltelefoni, programmerare, affärssystem, nätverkstekniker och så vidare. Det är ett gammalt 20 manna företag, om man tittar på vår dagliga business så är det ett 20 manna företag som jobbar med Malmö som bas. Så det är väldigt mycket middle-management, vi har inte 60 stycken Vd:ar och marknadschefer utan detta håller på att konsolideras. Så vi försöker styra upp en del

centrala funktioner men det är ganska stort arbete, så vi sitter och bidar vår tid. Man tänker väl att det ska hända mer än det gör. Man tror att man vet vad som är en bättre lösning men det är inte så snabbt fixat. (…) är i huvudsak en driftorganisation. Alla stora konton är GE-moneybank, Statoil och då är det en drift miljö. De har sina IT-system stående hos oss. Sen finns det andra saker, med 14000 anställda så har du all kompetens men det är väl drift som profilerar (…).

RH: Vad har (…) som organisation för syn på sociala nätverk?

R1: Väldigt dåliga direktiv. Vi har inte fått några styrningssignaler för vad som förväntas och inte. Tittar man på ledorden så när de lanserades för ett år sedan så var det nästan lite religiöst. Typ att jorden ska bli ett bättre ställe. Det har de dragit tillbaka nu och formulerat om så nu är det mer excellens och beyond expectations men fortfarande även ta hand om varandra. Bolaget vill profilera sig som att man ligger i framkant, och att vi ska ligga rätt i tiden och där inkluderas sociala medier. Jag har inte varit ute och tittat men jag tror inte det finns någon Facebook grupp, det finns heller inte någon som sitter och jobbar med sociala medier som en markadsföringskanal, verktyg eller för att kommunicera med de anställda. Det är inget jag har sett och det vet jag inte om det jobbas centralt med heller. Men det har heller inte kommit ut några policys. Det är ingen som har talat om vad vi får eller inte får göra. Huruvida vi får delta i forum när vi sitter på jobbet. Det är inte ens skrivet i papper. Vi 25 som sitter på (…) One Malmö skriver våra egna anställningsavtal och egna policys. De är ju säkert bättre än de som koncernen har. Om det finns någon koncernpolicy så är den inte kommunicerad.

MN: Det är inget som pushas ut till de anställda?

R1: Nej, det kan jag i min roll tycka är konstigt. Det är ju det jag driver på i mina kundrelationer. Men det är det gamla vanliga, att om det bara är 30-50 anställda så kan man ju lösa många problem genom att skriva ett papper. Men om man är 13000 anställda så är det ju svårt. Går man då in och bygger tekniska övervakningar blir det på andra hållet. Då blir det 13000 människor som frågar varför.

RH: Detta går kanske in på vad du svarat redan, men används sociala nätverk inom det dagliga arbetet?

R1: Ja, ni har kanske en annorlunda definition av sociala nätverk.

RH: Vi menar externa sociala nätverk vill vi vara tydliga med att säga. Facebook, Linkedin, Twitter.

R1: Det är inget företagsrelaterat, utan helt individstyrt. Bolaget har ett intranät men det är inget aktivt media. Det finns en massa information men det är den gamla klassiska strukturen. Man kan lägga upp information, foldrar där du kan dela information och låsa det till din verksamhet. De lägger upp lite nyhetsbrev. Det kom något blogginlägg från Vd:n. Intranätet lanserades i maj 2012 och det har kommit två inlägg. Man är ju inte där för att det händer en massa spännande. Däremot Lync, chatt och sådana kommunikatorer, det används väldigt mycket. Det är ju också externt men jag kan ju inte chatta med dig där hur som helst utan det kräver ju lite godkännande. Men som intern funktion så är den väldigt använd. Men allt annat, det är ju säkert massor som är med på Facebook och Twitter, och de skriver väl säkert företagskommentarer ibland. Och det är säkert anställda inom företaget som är vänner på olika håll och kanter. Men det är inget som är organiserat och styrt. Det är ingen som säger

vad man ska göra och inte göra. De som är aktiva privat kör säkert på jobbet men det är inget som är planerat.

MN: Kunskapsdelning, vissa företag använder sig av Wikis för att dela med sig av kunskap inom företaget. Om något varit med i ett projekt och lärt sig något kan det skrivas någonstans så andra kan använda det, finns något sådant?

R1: Nej, det finns en del gemensamma erfarenhetsdatabaser men det är inte uppdaterat. Om någon lägger information där så används det inte. I min professionella mening så är det inget jag saknar heller. Däremot om man jobbar med revision, de gör samma jobb hela tiden, lägger in samma rapporter hela tiden. De borde ha användning av detta. Det är ju samma sak år ut som år in, lite andra siffror bara. Kommer det en ny lag som förändrar hur man ska hantera något så ligger det ju i intresset för alla inom en bransch som drabbas av detta, och då vill man kanske ta fram om något gjort en revision eller lagt en kommentar. Men de använder det inte. Jag känner en massa folk där, de måste mata in en massa information hela tiden men så länge ingen gör något så är det inget värt. Vi har en CV databas där man ska kunna söka en kompentens. Men om man lägger in information så kan den säga att man har fyllt i den till 97 procent, och då har jag skrivit att jag tycker om att gå ut och gå med hunden som kompetens. Det är ingen som kontrollerar information. Jag tror det är likadant överallt. Ingen som styr och övervakar, jag kan göra vad jag vill. Jag tror inte att det är möjligt att göra en kompetensdatabas för 10000 anställda men vi som är här i Malmö, vi borde inte behöva hantera samma problem, när vi sätter upp en ny lösning.

RH: För att sammanfatta, det finns inga direkta riktlinjer varken för eller mot utan man får lov att använda för privat bruk?

R1: Var anställd skriver antagligen på ett avtal. Så detta har ju säkert en klausul om att man inte får lov att diskriminera och så vidare. Det är ju på papper skrivit då.

RH: Vet du om det uppstått problem av användande av sociala nätverk?

R1: Inte som jag känner till, inte via nätet.

RH: Främst ur säkerhetssynpunkt och inte i PR syfte då alltså.

R1: Om du tänker att det skulle vara några personuppgifter som kommer allmänheten till känna eller om det är någon som chattat eller twittrat i vårt namn så är det ingenting jag känner till, inga sådana skandaler. Inget jag har kommit i kontakt med i alla fall.

MN: Och inte heller någon sorts virus eller liknande som skadat organisationen på det viset?

R1: Nej, det har vi inte ens fått via traditionell IT heller. De gånger vi märker av driftstörningar som jag själv varit med om, det har ju varit tillfällen då Microsoft släpper en patch, som nu i tisdags. Så alla som körde Kasperskys antivirus, som vi gjorde och en av våra kunder, så drar den igång checkdisk när en enhet startas, så alla som startar om datorn får vänta i 5-6 minuter på att checkdisk ska köras. Detta får ju en inverkan, framförallt för admin personal. Tekniker undviker problemet. Men alla som inte är vana, de sitter där. Och när de startar datorn hos kund får de vänta 5-6 minuter på att det ska starta. Det kostar ju pengar och blir problematiskt. Det har väl hänt två eller tre gånger de sista åren. Det är ju ett av de få centrala direktiven som har kommit ut, att alla skulle installera bevakningsmjukvara, Absolute

software. Jag vet inte om ni är bekanta med det, men i alla datorer finns det inbyggt på chipnivå en kontrollfunktion som normalt är inaktiverad av leverantören. Men kunder kan köpa programvara som aktiverar kontrollfunktionen. Den läser av allt som finns på datorn, programlicenser, när du kopplar upp dig, om du kör trådlöst eller aktivera GPS funktioner om du har det i datorn. Säkerhetsmässigt kan du kontrollera datorn så om du går utanför vissa geografiska domäner så kan du låsa datorn. Detta är något som är inköpt centralt. Men om du har en decentraliserad organisation, ge dig inte på att centralisera någon lösning utan att ha central support eller hantering. För om du har 10000 anställda som är vana att sköta sig själva och du helt plötsligt säger att nu ska alla installera den här mjukvaran så kommer det att hända grejer. Och de som det händer hos, de vill ha någon att ringa upp och skälla på och klaga. Och vi som sitter här, jag kan ju gå till min tekniker. När han frågar mig varför jag installerat det här programmet, så säger jag att det har de ju sagt uppe i Husqvarna, men då svarar han att jag får ringa till dem då. Och så pratar man med dem och de hänvisar vidare och så slutar det med att man sitter och pratar med sin interna servicedesk.

RH: Ni har konsultverksamhet och då sitter ni antagligen ute hos kund med kundens dator och information. Hur säkerställer ni att data förvaras på ett bra och säkert sätt?

R1: Det enkla svaret är att det inte är vi som bestämmer det utan det är kunden. Om inte kunden ställer krav på hur vi hanterar deras information så har vi inga krav på det. Sen finns det olika nivåer. Vi har tekniker man-på-plats, enkelt uttryckt. Ett bolag som är mellan 20-100 anställda, så är det ovanligt att de har en anställd tekniker för det är inte 8 timmar arbete om dagen. Så då kommer vi in med en lista en eller två gånger i veckan och gör det. Då är det actionlists som man gör på plats och det är ju allt från övervaka servermiljö, backuper, kollar klienter, användarsupport och så vidare. Det är ju ganska brett område. Det vi frågar efter det är: Vart är ni på väg? Det är ju inte tekniken som kostar pengar utan ni som verksamhet, vad är det ni tjänar pengar på? Så man vill få reda på nyckelprocesser, är det försäljning, logistik eller ekonomi. Det kan vara vad som helst och det behöver inte ha någon koppling till IT system i sig självt men alla är ju beroende av IT-system i någon mening. Det är ju steg två, innan ett företag vet vad deras nyckelfaktorer är för deras framgång och innan man identifierar vad det är som ska fungera, det är inte förrän då som en tekniker kan gå in och göra en analys. Detta kan vara att man ligger lite efter på de här två punkterna eller att man har overkill här med redundanta diskar och speglade system. Men vad är det som backas, är det bara bilder och gamla dokument som de inte använder i det dagliga arbetet. Och så har de byggt sådana jävla system att det inte ska ligga nere mer än 10 sekunder. Varför då, ni kan ju vara av med den här informationen i två dagar, varför betalar ni 50000 kr i månaden för detta. Och sen att synka mobilen, det är ju skitviktigt. Så fort någon chef är ute och reser och de tappar synken, tappar VPN, ja då plötsligt börjar det ticka pengar. Men det har de inte specificerat, hur det är tänkt att fungera, hur och var. Det är de stora riskerna och där jobbar jag mycket med kunderna och försöker få upp en medvetenhet. Vad är det som ska fungera och hur mycket får det kosta.

RH: Det kan bli upprepande av frågor. Men hur ser er säkerhetspolicy ut?

R1: Vi har väldigt långt gångna säkerhetsrutiner vad gäller access till lokaler och fysisk säkerhet. Ni kommer inte in här utan att någon öppnar dörren för er och ni får inte komma in om ni inte har en [namn]lapp på er. Jag kan inte gå med mitt kort i alla våra lokaler, jag kan inte komma in på drift avdelningen. På samma sätt är de som sitter med Active directory, backupper eller klient, de har olika roller och olika behörigheter. Så de kommer inte åt systemen heller. De som sitter i serverhallen får lämna över brottsregister, och man ska ha gått

utbildning och blivit certifierad annars får man inte åtkomst dit. Det är samma med servicedesken, de sitter med lite för höga rättigheter till de olika kundsystemen. Där skulle man kanske också ha ett lås så man inte kunde gå fram och tillbaka. Där är vi långt gångna, med sekretess och allt sådant. Men jag kan bara svara för här i Malmö, jag vet inte hur det ser ut i Anderstorp. Men min största angelägenhet gällande sociala medier, molntjänster och internet överhuvudtaget, är att när du släpper iväg information som är företagets, vem äger den informationen. Det är det ingen som satt ner. Om man går in här så även om de styrt upp så är det nog väldigt många som kan hitta ett admin lösen och via det har åtkomst till system som de inte borde ha. Då finns det något som heter kompletterande kontroller, om man lägger in loggar eller lägger in manuell uppföljning i systemet så kan man logga trafiken och verifiera bakvägen att det inte varit någon inne. Tittar man istället på information ut på nätet. Jag satt på ett projekt för fem år sedan då ett svenskt bolag skulle köpas av ett amerikanskt/engelskt, ett migreringprojekt. Då kom ekonomichefen efter två månader och frågade var JD Edwards, det nya ekonomisystemet, rent geografiskt. Det driftades i någon serverhall uppe i Oregon (Amerika), men det fanns lagar och förordningar att ekonomisk information inte får lagras utanför EU:s gränser om du inte har skattemyndighetens godkännande. Inom EU så har man ett antal krav som ska efterlevas, då är det good-enough, men lämnar man EU, då är det helt andra krav. Och sådant vet inte folk om förrän det händer. I någon undersökning av studenter jag sett, antagligen amerikanska, på något universitet, var 98 procent aktiva på internet, 95 procent hade en presence via Facebook eller Twitter, 93 procent mobiltelefon och 60 procent, en ganska hög siffra, som var aktiva bloggare eller twittrare, och inte bara läser utan skriver saker också. Det är klart att när den här armadan kommer ut så kommer de att fråga varför kör vi inte marknadsföring via Facebook, eller kundkontakter. Och då säger jag fine, men när vi släpper den här informationen, var hamnar den? Är det din, företagets eller kundens. Och när den släpps, vem har åtkomst. Även om det är molnet så finns det några servrar någonstans där denna information ligger. Där finns administratörer och andra som kan komma åt det. Hur är det säkerställt? Och när det går in i driftläge, vad krävs. Det är ju väldigt omoget. Det funkar ju på Facebook med musikgrupper släpper lite musik och lägger upp spelningar och så bygger man upp en massa vänner. Men de verksamheter jag känner till, det är små bolag, bygger kontaktnät, lägger roliga grejer och det funkar nog rätt bra. Men då är det här gamla, när något går snett, om det här bandet gör en disaster konsert då sprids det som en löpeld och det kanske till och med sprids på deras egen site. Det är ju snabbt gjort att lägga upp information men du måste söka upp den och jobba med den och det finns inga färdiga processer för det. Jag tror det är annorlunda om ni går och tittar på någon som utvecklar spel. De bolagen är inte 10 år gamla. När de satte igång fanns redan internet och Facebook. Då är det lite mer inbyggt så där kan jag mycket väl se att det ser annorlunda ut.

MN: Men för er organisation så känner du att det skulle behövas mer kontroll för att kunna använda det?

R1: Jag tror inte det finns kompetens. Jag är utbildad ekonom, jag gick tekniskt gymnasium. 93-94 började jag jobba på riktigt, 20 år sedan. Då fanns inte internet. Det var ett tomt skrivet blad. Första Arpanet när Lunds universitet drog igång, då fick man gå in med dospromt, skriva in kommando och koppla upp sig mot IP nummer. När det kom textfiler sen var det jävligt imponerande att kunna hämta dem från ett annat universitet. Jag bedömer mig själv som ganska IT-mogen trots att jag jobbat mer med revision och kontroll. Men alla som är chefer idag, de är min ålder och 10-15 år till, de har ju lägre/sämre IT-mognad. Då när vi pluggade på 80 och 90 talet, det var inte som läste IT. Det hette ju något sånt som BAS eller något. Det är ju ändå de som är chefer och Vd:ar som styr bolag, lägger upp tre års strategier

idag. Det är inte så moget om man tittar i affärsverksamhet. Sen bristerna. Om ni tar Framfab, när de sätter sig på Ericsson och ska leverera sina kittade internettjänster då sitter de inne på Ericssons mobiltelefoniutveckling. En sådan här rackare (iPhone) skulle ta 6-9 månader. Du passerar inte första nålsögat förrän denna här dokumentationen är klar, dessa tester genomförda och denna approval gjord, för nästa gäng måste veta att allt funkar som det ska. Och så glider det vidare med stöttest, funktionstest och batteri. Och sen innan det ska in i produktion ska det planeras leverans av chips och grejer från Japan. Det var stenhårda protokoll. Och detta skulle göras på nio månader. Du kunde inte sitta och vila på hanen när du ska ha produktion om nio månader. Du måste sätta igång redan då och planera för inköp, logistik, leverans, marknadsinformation som ska typgodkändas. Och så kommer fleecetröjorna in (Framfab) och säger att de ska köra på internet så löser det alla problem. Vi kan leverera via en webb shop. Direktörerna med vita skjortor och slipsar, de säger vad snackar ni om. Och så sitter de (Framfab) och säger gamla stofiler. Så skrev de någon utredning och Ericsson skickade tillbaka den med rödmarkerat överallt, typ gå hem, gör om, gör rätt. Sen tre månader senare hade de ett lösningsförslag som Ericsson kunde acceptera, vi pratar alltså om intranät, då kom en faktura på 150000 kommer jag ihåg att de berättade därför de hade gjort kompletteringar. Vi (Ericsson) har ju utbildat er i hur man sätter upp en projektplan. Det här kommer ju krävas för sociala medier, cloud och allting. Det är omoget. Om 10 år är det säkert ingenting konstigt men idag finns ingen process som är färdig. Gör de här stegen så vet du att du kommer att få en fungerande process. Om det är ett nytt företag som bara vill sälja (med hjälp av sociala medier) hur fungerar reklamation. Det finns ju lagtext, om de köper via nätet var ska de reklamera. Övervakning av kreditkort och personuppgifter och allt sådant. Man kan ju köpa den tjänsten via någon länk nånstans. Du kommer hitta många småbolag som gör det men du kommer inte hitta några stora. När EON tecknar ett avtal med sin processstyrningsleverantör då tecknar de ett som löper i 20 år. Du bygger inte ett vattenkraftverk för att du ska uppgradera det varje tisdag eller utveckla det och sen köpa nytt om tre år. Det ska stå där i hundra år. Någon trycker på en knapp i Malmö och så är det i praktiken en lucka som öppnas en centimeter till för att öka energiproduktionen. När de tecknade dessa avtal på 90 talet skrev de in att de inte fick uppgradera systemen. Så länge det inte är isolerade system så är det ok men de som sitter och jobbar på ett kärnkraftverk vill också surfa på internet och så måste man ha två separata nät eller kan man ha en brandvägg. Den brandvägg som särskiljer ett publikt nät till ett kärnkraftverks processnät, det räcker inte med good enough. Det duger inte med en mjukvarubrandvägg, det finns ingen mjukvara som är säker. Då får man hårdvarukryptera eller ha fysiskt skilda nät.

RH: Så ni har ingen del i er policy som behandlar sociala medier. Men ni har en säkerhetspolicy?

R1: Jag skulle säga att den policy som finns är: Under eget ansvar, När du kommunicerar på internet så gör du det i företagets namn. Beställer jag en resa eller om jag gör ett inlägg på någon chatt eller om jag har skrivit någon kommentar på aftonbladet så är spårbarheten direkt pekad på IP-nummer eller en adress som pekar hit. Vilket innebär att då är det (…) som står för det här och detta måste man vara medveten om. Men våra interna policys de har ju inte då slängts omkull, de förbjuder oss inte att vi får beställa flygplansresor, vi får lägga spel på Lotto. Vi får göra sådana saker. Vi får titta på Youtube och så vidare då. Men vi får inte skriva rasistiska inlägg, vi får inte sitta och tanka hem filmer och vi får inte begå olagligheter. Men detta är bara på papper, tekniskt sätt så kan vi göra det. Det finns möjlighet till övervakning, det är väl ungefär vad som står. Om polisen ringer till oss och säger att vi misstänker att det pågår brottsliga handlingar, då finns det ju möjlighet att logga i trafik, det finns det ju alltid. Men sen var man får och inte får gör och hur du kan hamna in the court of

law det vågar inte jag gå in på. Jag har jobbat en del med jurister också, men då är det traditionellt. Det finns ingen lagstiftning som styr vad du får och inte får göra över internet, alltså det är prejudikat och sådant. Vi får se. Någon får anmäla någon och sen så blir det fomslut och när det domslutet är satt så har man en prejudikat till nästa gång någon gör samma sak. Och sen utveklas det om det händer ofta eller om det är svårtolkat så sätter man sig och börjar skapa nya lagar, men det där är ju en tioårsprocess.

[Mailad i efterhand, skriftligt svar]: Har ni en del i policyn för sociala medier eller är den allmän? Hur skapades den? (Ramverk, ex. CoBIT, av ledning, överenskommelse bland anställda?)

R1: Gällande din kompletterande fråga idag har vi naturligtvis standard tekniskt skydd i form av FW, Antivirus och monitoring och i samband med detta. Vid större fel eller om det sprids kunskap kring nya virus, hanteras detta alltså av tekniker. Sedan finns i vår (vi 17 i Malmö alltså) allmänna policy inskrivet standardformuleringar i form av att man inte skall öppna mail från okända avsändare, inte klicka på länkar eller utföra instruktioner för att öka säkerheten osv. och även att vi vid misstanke om oegentligheter, malware eller annat ”misstänkt” skall rapportera detta till närmsta chef för uppföljning. Men inte mer än så.

RH: Vem är det som ansvarar för er policy eller det som ni ska tänka på? Är det på koncernnivå?

R1: Nej, jag skulle säga att det är vi själva som bestämmer. Det ser nog annorlunda ut beroende på juridisk enhet. Outsourcing har en egen kille. Jag tror de är hårdare än vad vi är. De har en bok som är 80 sidor och den ska alla anställda ha läst och förstått, jag tror till och med de har ett litet onlinetest där man ska svara på en del frågor där du ska ha 80 procent rätt eller något sådant, för annars får du backning. Eller så tappar du inte får ha vissa konton om du inte kan det. På vår avdelning så jobbar vi med det ute hos kund, våra tekniker är mera självgående och när vi sitter här inne så sitter vi ju i en driftmiljö. Vi har ju tiotusen användare som gör samma sak. Då ör det enkelt att standardisera. Alla kör Outlook, alla kör Lync, alla kör de programmen. Men våra killar, de är ute hos 40 olika kunder. De 40 kunderna, de kör Mac, de kör, något annat system, de kör Outlook, någon kör något annat system via nätet, någon som har tio år gamla maskiner. Våra killar kan inte gå ut med en standard plattform och jobba för då kan de endast jobba åt två av kunderna.

RH: Men tror du att säkerhetstänket kring det här med policyn och sociala nätverk har förändrats sedan området blivit större och har det haft inverkan på policyhanteringen?

R1: Nej, jag tror man möjligen har lagt till något som saknas. Om man säger säkerhet, om man talar om för folk vad de får och inte får göra så är det man ofta glömmer bort konsekvenserna. Det är ju enkelt att skriva en policy, då får inte [göra någon sak], men vad blir konsekvensen om jag ändå gör det. Och där är folk dåliga, det är som en backup. Man installerar den och så testar man den, men vet man om det är rätt information och kan man återställa det så som man tror att man kan?

RH: Du menar att det inte är någon kontroll på om den efterföljs?

R1: Nej, och jag tror det är samma sak här. Om det nu är så att du får inte skriva rasistiskt inlägg. Om nu någon ändå gör det så händer det ingenting för det är inget som upptäcker det.

Men om någon skulle upptäcka det och får någon publicering inom TV ja då blir det ju helt plötsligt en het potatis. Jag tror att det enda tillägget som du gjort nu är att du har skrivit till i de här avtalen att om du inte efterlever policy så kan du få sparken eller så kan du bli polisanmäld och det har inte stått förut. Tidigare har det bara stått att du ska göra någonting, som att redovisa tid för att ta en vanlig enkel sak. Så jag tror formuleringen är ja det är ingen som installerar några övervakningsmedier, men vissa verksamheter spärrar naturligtvis, men vi är en flexibel organisation som jobbar med många olika kunder och vi kan inte låsa oss. Sitter du och jobbar på Försvaret, Luftfartsverket eller Eon då är det ju spärrat och är det ju non-negotiable. Där finns ingen där som kan begära en öppning till Svenska Spel, därför det kommer aldrig att gå igenom. Men det styrs väldigt mycket mer än andra verksamheter.

RH: Innehåller er säkerhetspolicy speciella riktlinjer för hur de anställda får använda sociala nätverk?

R1: Det kommer sakta men säkert. Om du tittar på mobiltelefoni som en del så har vi ett företag som heter "Lesswire" inom koncernen. De jobbar med ett management-verktyg. Det är ingenting som implementerat idag, jag kan installera vilka appar jag vill på min mobiltelefon. Jag kan söka, surfa, mail, och så vidare. Men det kommer komma in, tror jag och det är bara ren allmänhälsa. Koncernen är ju inne i en omstrukturering nu och det är rätt jobbigt att föra in nya lösningar, men mobiltelefoni är ganska enkelt i sin tillämpning, men jag tror det kommer vara så att: Om du blir anställ på (…) så kommer du köpa en av de här två telefonerna. Och då kan du antingen bli en vilde, det innebär att då kanske du måste leva upp till vissa policyförändringar eller så stänger man av vissa tjänster så du inte kan koppla upp dig på det lokala nätverket eller liknande. Vi har ju ett sådant gästnätverk och det brukar ju vara bakdörren. Det är som att ni har stadsnätet och får ett konto, det är fritt blås. Vi har på motsvarande sätt gästnätverk så när kunder kommer hit så kan de koppla upp sig här mot (…)guest och logga på, men vad ni gör där är upp till er. Ni är ju aldrig inne på vårt nätverk. Men med de här verktygen då är det just viruskontroll, du ska kunna låsa telefoner, du ska kunna ta bort information på telefoner och de som sitter i de positionerna och det är väl egentligen förarbetet som måste göras. Vilka är det som är målgruppen. Det är ju en dyr lösning om du ska implementera det på tiotusen, men säg att det är femhundra som är den här riskgruppen. Ta min telefon, jag har inga hemligheter på den, inte i mitt jobb så att säga. Men det kommer säkert det här Absolute Software det är klockrent också. Där kan du verkligen styra vad man gör och inte gör på en dator som tillhör företaget. Men vi är inte där än. Det här är skitbra program, skulle ni få en demonstration och gå in och titta vad man kan göra med de här. Hade jag startat ett nytt bolag som inte har tiotusen anställda så hade jag implementerat det som en standard direkt. Tagit fram nödvändiga styrdokument, utbildat personal, ni använder det på det här sättet där för att om man får in det i en organisation så är det ju inte så konstigt även om man växer och bli tiotusen, så kommer det fortfarande vara en hanterbart. Men när du har tiotusen olika, den dagen de trycker ut så att du helt plötsligt inte kan använda din telefon så som du kunde göra igår. Då har man inte tekniska problem men användarproblem.

RH: Hur kontrollerar ni att policyn efterföljs?

R1: Vi levererar bättre kvalitet till våra kunder än vad vi själva gör. Ute hos kunder så har vi installerat övervakningssystem som larmar. De skannar av nät, kollar farliga programvaror, statistik på trafik som åker in och ut. Det har ju två funktioner, det viktigaste är ju att man ska ha något early warning system rent prestandafunktionsmässigt, det har inte med säkerheten att göra. Vi tror inte att våra kunder drabbas av intrång för att det är någon som försöker hacka

oss, för de som sysslar med sånt skjuter inte in sig på den typen av verksamheter. För några år sen var det ganska populärt att hacka allt skit man kunde komma åt, men det var ju för att man skulle sno processorkraft och så. Så det var inte information som var intressant utan att komma åt så mycket dataresurser som möjligt. Så den dagen då du skulle göra något så sköt du från en miljon olika ställen. Hotbilden ser ju olika ut för olika bolag. Vi har mycket tillverkning[företag], men de firmorna som är mellan 20 och 100 de är ofta de som har funnits i 20-30 år och tillverkar kläder eller gardiner. Eller så är de konsultföretag som jobbar med rekrytering är tillverkningsföretag för plast, stål, och så vidare. De jag bli mest förvånad över att de inte själva drar i den här typen av frågor är rekryteringsbolag. De gör alltså uppdrag åt Ericsson och de stora bolagen och det är chefer de rekryterar. De om några borde ju sitt på känslig information som de inte vill ska slippa ut. jag hade ju satt säkerhetsnivån betydlig högre än på ett tillverkningsbolag av plast, där hade jag mer fokuserat på drift. Men internt så har vi det väl lite sämre. Vi är tyvärr reaktiva i vår enhet. Det finns loggar och system som övervakar men det är ingen som aktivt arbetar med det där. Vi lever lite som kunder. Vi litar på oss själva och på våra anställda.

RH: Men skulle du säga att nyttan med sociala nätverk väger upp riskerna som kan komma med hoten i användningen?

R1: jag tror det beror på verksamheten. Jag tror inte att ett företag som tillverkar plast och säljer till agenter, som inte är slutkunder, som de levererar till utan de är underleverantörer tillhusbyggen. De har fem-sex kunder som står för 90 procent av deras verksamhet. Jag tror inte att de breddar sin verksamhet genom att vara närvarande på sociala medier. Eftersom det bara finns risk där så ser inte jag någon anledning.

MN: Om det är företag som är med B2C?

R1: Alla bolag som vill synas som ser ett värde i att man profilerar varumärket måste ju vara intresserade av att delta. Även om det inte säljer prylar. Och där tycker jag att (…) borde vara mer intresserade av att finnas närvarande och promota lika väl som att man har telefonnummer och mailadress på ett visitkort. Är du på en mässa eller om du gjort ett kundbesök, att ha flera referenser som är lite mer närvarande. Det kan ju jag tycka känns givet att man ska ha. Men lika givet känns det som att då måste man ha ett gäng sitt någonstans som ansvarar för (…) och deras problem eller utmaning i dagsläget skulle ju vara: Hur ska vi promota (…)? (…) är så mycket och stort. Vi kan inte bara pusha ut loggan. Och är det så att vi deltar i någon mässa och alla mässorna är snortunga gällande outsourcing och drift och backup. Då skrämmer vi bort massa kunder som går in på vår Facebook-sida och ser att vi bara ställer upp på sådana mässor. är du inte ett företag med 3000 mannabolag som letar efter outsourcing, så går du inte till (…). Vi sitter ju med affärsutvecklare, systemutvecklare, vi jobbar inom medicin, inom skog, och det är det som är problemet med hur fan du profilerar en korrekt bild av verksamheten. Man måste veta den strategin och processen. Jag ser framför mig att det här är enklare när du har Hofbro Haus där är jag [Facebook]vän. De säljer mat och öl i Tyskland på ett ställe. Alltså på lördag så spelar de och nu är det tre veckor kvar till oktoberfesten kom och se. Det är så enkelt att köra den. Det funkar ju inte på (…). Det är enklare om man har ett fotbollslag, alltså kräng souvenirer och prylar och vi spelar fotboll. Musik, senaste konserten, man har köpt CD-skivor. Jag vet inte men uppföljningsbiten där och processen, vad är det vi vill ha ut och hur mäter vi framgång. Hur ser vi om vi får någon feedback. Det kanske är viktigare att ta exemplet om detta är rätta stället att arbeta på och skapa ett forum som mer vänder sig till potentiella anställda. Om du tänker dig: Hur trivs personalen på (…). Vi skiter i vad vi levererar, vi jobbar med det ena och det andra, men vi

kanske ska ha något som i Köpenhamn där det går en stafett där du anmäler dig. Vi är ett gäng som bussar ner till oktoberfest finns det fler (…)-anställda som vill vara med? Nu går vi på en kampanj, är det fler som är intresserade. Om det är någon som drar igång en utbildning i sociala medier. Det kanske sitter 100 stycken som skulle vilja gå den här utbildningen. Men eftersom de är en här, en där och en där, så blir det aldrig av. Men om vi säger att vi hyr in en kille till Karlstad i tre dagar, vi kan ta 40 man. Det kanske kommer 40 man, men den kanalen finns inte. Där skulle man kanske ha ett större värde av sociala medier. Det har ju inget med själva verksamheten att göra. Men det är nog lite det där man får analysera lite. När man använder sociala medier, vad är det man skriver. Glöm att som vad man käkat till lunch eller varit på Sats och sådär. Men om jag ska åka till Proto och är intresserad av portvin, är det någon som varit där och kan något om portvin så får man ju svar direkt av ett par stycken som ofta har något att komma med. Då blir det ju ett värde.

RH: Märker ni eller gör ni någon skillnad på olika kunder beträffande säkerhetshanteringen

R1: Ja, det är stor skillnad.

RH: Får ni rätta er efter kundernas policy?

R1: Nej. Vi har ju G4S och de ställer ju krav och då är det enkelt att leverera. Det är som jag sa förut: Det är upp till kunden. Det är det enkla svaret. Problemet hos kunderna är att beställa kompetens. De kan ingenting. Det är förvånansvärt låg beställarkompetens inom vissa områden. Men då är det lite som jag säger. Jag är 47 år gammal, jag har jobbat i 20 år drygt inom branschen, jag är en ganska bra beställare. Men de som är VD, ekonomichefer eller administrativa chefer som blir CIO (Chief Information Officer), de kan inget om IT på det sättet. Ännu värre är att man under hela 90-talet byggde egna system och man hade gigantiska serverhallar och under 2000-talet så har man ju flyttat ut de här grejerna och vad har hänt då? Jo de som jobbade med det här har fått sparken och så ska de effektivisera och flytta. När vi ställer frågor om hur de hanterar sina Microsoftlicenser så är det ingen som vet det. Inte en som är chef för 2000 man vet hur de hanterar licenser. Vad har ni för applikationer? Egenutvecklade applikationer som gamla special mätverktyg förväntar sig kunden att vi kan(!) bara för att vi är ett IT-bolag. Ska vi kunna det? Deras egen kompetens har utarmats under flera år då de först varit en del i E-On och sen har de här programmen bara legat och snurrat i tre år. Och nu när de ska upp på en Windows 7-platta då är det ingen som har en aning.

MN: Så då får ni peka ut för dem vad de behöver fokusera på?

R1: Det vet vi ju inte heller. Vi ställer ju bara kraven, vem är leverantör? Ja det var Olle i Linköping, men jag tror inte han jobbar längre. Alltså, ni skrattar men this is life. Men det är generellt sett är beställarkompetensen på kundsidan låg. Det som är medvetna, alltså G4S, E-On, banker och myndigheter är inga problem. De kommer till oss och visar IT-strategin, så här ser våra policys ut, implementera. VPN så ska ni använda den här programvaran och konfigurera den så här och det ska fungera så här. Då behöver man bara installera och testa. Men alla som växer in där internet smyger sig på. Mobilsynk, mobilitet, tillgänglighet, sker på bekostnad av kontroll så enkelt är det. Ju mer tillgänglig information blir desto mindre kontroll har de. De är inte med, de lägger upp information utan att veta vad det innebär. Det är som en femtonåring som sitter och skriver på Facebook och skriver: "Fan vad tråkigt jag har på jobbet". Hur kan man skriva så, din arbetsgivare ser ju det. Lite så är det på beställarsidan och speciellt när vi säger säkerhet. Vad innebär sociala medier? De vet ju inte och vi har ju

inga färdiga processer. Det är en gråzon. Alla sådana säkerhetsfrågor. Ställer du en fråga angående kraven så vet de inte. Ni hanterar ju sopor, är det inga miljökrav? Jo visst. Vad innebär det då? Vi måste skicka en rapport en gång i månaden på dessa saker. Om den informationen försvinner eller om den blir korrupt, vad får det för inverkan? Det vet vi inte. Det kan ju bli vitesföreläggande i miljonkronorsklassen och sen ligger det i en Excel-fil på en linux-burk som har stått där i tolv år. De har inte tänket. Excelarket började levereras 1998 sen har det gjort det i tolv år. Det är inga som vet mer och det har ju fungerat. Det var en snubbe inne i Arlöv, han startade ett mätverktyg för elmätare som man har hemma i huset i källaren och så när han testar det med jämna mellanrum så startar han systemet med en floppy disk på 8 tum. Har ni ens sett en sådan? Googlar ni på den så ser ni att den sista tillverkningen var vid 1976 på IBM. Han hade inga Å, Ä, Ö när vi körde DOS-prompten så när han skulle köra kommandoprompten i Windows 7 så fick han inte med typsnittet för dem, och det var hans problem.

Transkribering R2

MN: Vilken befattning har du?

R2: Marknadschef för (…) Sverige

MN: Vilka arbetsuppgifter har du?

R2: (…) är uppbyggt med ett gruppbolag i toppen och sen finns det tre bolag under. På gruppnivån är jag ansvarig för marknadssidan utåt för gruppen som helhet. Så det handlar om att se till hur vi syns utåt som helhet. Sen har varje bolag ansvarsområde själva också. Så jag har det övergripande ansvaret.

MN: Du har beskrivet lite om verksamheten men du kan kanske beskriva mer om vad ni gör?

R2: Vi är ett IT-konsult företag som fokuserar på tre områden, säkerhetsbranschen, automation och digitalmedia det vill säga webbmedia branschen.

MN: Så inom säkerhetsbranschen så är ni ute hos kund och säkrar system och så vidare?

R2: Ja precis. Vi säljer inga system, utan vi är konsulter hos bolagen och ser till att deras lösningar är säkert genomförda, tar hand om strategier, hur man sätter upp deras miljöer.

MN: Sitter ni på kunders data?

R2: Det är olika. Ibland gör vi det, ibland inte. Ganska ofta har vi access till kundens data.

MN: Vad har (…) för syn på sociala nätverk, och hur använder ni det?

R2: Vi kan bryta upp det i lite olika frågor. Vår generella syn på det är att som bolag så använder vi det sparsamt. Vi använder Facebook, Twitter och LinkedIn som våra främsta kanaler. De har lite olika syften beroende på vilket det är. Men framförallt så är de som rekryteringskanaler. Det handlar om att visa upp vilken arbetsgivare vi är. Det handlar inte så mycket om dialog och kommunikation för vi har inte så mycket folk som driver det här egentligen

MN: Så det är mest för att hitta potentiella anställda?

R2: Ja precis. Vårt närvarande på LinkedIn gör vi genom att ha kampanjer, vi har vårt alumni och en företagsprofil. Facebook är mer för att pusha ut vad vi gör. Som IT-konsultbolag så har man inte en stor skara följare. Det är ju naturen. Så det blir mycket att pusha ut att vi har föredrag där och nu händer det här och det här. Det är främst (…) som håller till där.

RH: Så LinkedIn är mer riktat åt er framtida arbetskraft?

R2: Precis

RH: Och det andra är mer åt potentiella kunder?

R2: Nja, lite mer inåt företaget egentligen för vi får ju inte så många kunder som följer oss på Facebook.

MN: Vad menar du in mot företaget?

R2: I och med att det är så många av oss som är med där blir det ett sätt att sprida information inom bolaget. Vi finns ju på många platser i Sverige och då är det en snabb kanal att få ut information.

MN: Är det tvåvägsinformation eller är det information ni lägger upp som andra tar del av?

R2: Facebook är framförallt envägsinformation. Sen har vi interna system som är tvåvägsinformation, som Yammer. Där är det med full dialog. Men då är det ett slutet nätverk inom bolaget. Så det är inte ett socialt öppet utåt utan socialt inom bolaget.

MN: Hur ser ni på anställdas användande av sociala nätverk för privat bruk.

R2: Det ser vi klart positivt på. Det är snarare den vägen vi vill gå. Vi som bolag kan inte vara den som går ut och pumpar ut information utan det får ske på individnivå. Vi är såpass stora och så pass splittrade i det vi gör, så vi som bolag kan inte gå ut och pinpointa expertkunskap utan det är bättre att den som kan det får göra det.

MN: Du har redan svarat på det till viss del men används sociala nätverk till det dagliga arbetet inom organisationen?

R2: Det gör det, och sen har vi ett par personer som är talespersoner och det ingår i deras arbetsuppgifter att vara aktiva utåt i sociala media. Det gör det i sitt eget namn men under flaggan (…).

RH: Är de ansvariga för det som skrivs om (…)?

R2: Det är de som är inne och skriver där. Men det är del i deras uppgifter att driva den personliga plattformen framåt också.

MN: Har det någon gång uppstått problem av anställdas användande av sociala medier?

R2: Inte än.

MN: Har ni någon slags utbildning för anställda hur de ska agera eller någon slags direktiv?

R2: Nej det har vi inte. Det är sunt förnuft, vi kör IBM linjen.

MN: Vad betyder det?

R2: IBM gick ut och satte i sin policy att i princip, inget naket. Annars gör vad ni vill.

MN: Hur säkerställer ni kunders data, vad har ni för riktlinjer?

R2: Ofta när vi hanterar kunddata så följer det med ett NDA, ett avtal, som det står att vi inte få lämna ut den här datan. Så följer det med riktlinjer för hur den får hanteras och vem som

får hantera den. Ibland är de personliga och ibland på bolagsnivå. Och utifrån den får vi riktlinjer för hur vi får använda den, hur den ska sparas, vem som får se den.

MN: Så det är kunden som bestämmer så följer ni kundens önskan.

R2: Ja precis. Och ibland så ligger datan på kundens server, då har vi ett VPN ni och kan access:a datan där. Ibland behöver jag databaserna här så då får vi följa vissa regler för hur den ska hanteras, hur den ska sparas. Vi har en serverhall här, hur ska vi låsa in dem på rätt sätt.

MN: Och vem som har tillgång till dem?

R2: Ja precis.

MN: Har ni en säkerhetspolicy för IT, en generell IT policy.

R2: Ja i och med att en del av oss är säkerhetskonsulter finns det en policy för vad vi får göra och hur vi får göra saker. Den styrs av vårt interna IT i Göteborg som styr uppläggningen av saker. Dels så har vi skalskyddet utåt, med brandväggar som kontrollerar vad som släpps igenom. Vi är ganska öppna i och med att som konsulter behöver vi access till ganska mycket saker. Så det finns ingen nedlåsning av portar eller åtkomster till hemsidor. Men det finns policys för hur man kan access:a nätverket utifrån in och in. Det är samma sak här att vi får använda sunt förnuft för vad vi får access:a för sidor.

MN: I den säkerhetspolicyn, har ni någonting om sociala medier?

R2: Nej det har vi inte.

RH: Tror du att det är något som kommer att komma med tiden eller tror du att (…) kommer att förlita sig på de anställda som sitter med sociala medier?

R2: Jag tror att det kommer att vara som det är nu. I och med att vi är konsulter och sitter rätt mycket ute hos kunderna så handlar det väldigt mycket om att ta det personliga ansvaret som konsult. Och vi har väl inte sett något behov än av att sätta upp riktlinjer. Kommer vi till den punkten så får vi göra det men jag tror inte det kommer att behövas.

MN: Får jag fråga hur många anställda ni är?

R2: Totalt är vi ungefär 200.

MN: Och här i Malmö?

R2: Ungefär 20-25. I och med att vi sitter ute hos kund är det kundens regler vad som gäller på arbetsplatsen. Stänger de ner portarna för Facebook, ja då är det stängt. Så vi går ju oftast under deras regler.

MN: Måste ni följa deras policy gällande sociala medier?

R2: Om vi sitter på plats hos kund är det ju deras regler som gäller. Vi måste ju följa deras säkerhetspolicys. Vad kan vi access:a, hur kan vi prata om saker utåt. Där får man vara väldigt försiktig om vad man nämner på sociala medier om kunden.

MN: För de personer som för er talan på sociala medier, finns det någon kommunikation för hur det ska gå till?

R2: Det finns en grupp som består av mig, talespersonerna och ett par andra som är de som har rätt att i (…) namn gå ut och säga saker. Och samordnarna mellan dessa personer så sätter vi upp riktlinjer om det behövs.

MN: Vem inom organisationen ansvarar för uppdatering och implementering av policyn.

R2: Om vi haft en hade det varit jag tillsammans med talespersonerna.

MN: Men för säkerhetspolycin?

R2: För säkerhetspolicyn speciellt så är det uppe på ledningsnivå.

RH: Eftersom ni inte har någon policy for sociala nätverk är det något som sitter i väggarna, att man har vett och förstånd och att det är något de anställda vuxit in i förståelsen för det?

R2: I viss mån så sitter det i väggarna. Jag tror att mycket av det kommer av att man inom konsultbranschen sitter ute hos kunder vilket ger en naturlig följd av hur man ska använda sociala media. Om man sitter ute hos kund i ett landskap är det rätt naturligt att man inte sitter och R2bbar på fel sätt i sociala medier. Det är ganska uppenbart direkt.

MN: Har ni några speciella riktlinjer för hur anställda får använda sociala nätverk på olika enheter som BYOD, företagets datorer eller andra mobila enheter?

R2: Inte direkt. Vi uppmuntrar ju BYOD. Och det ingår i många personers arbetsvardag att ha kontakt över sociala medier så vi uppmuntrar det så gott det går. Vi ser ju att man blir ju oftare effektivare om man får R2bba fritt med det. Många har ju ett kontaktnätverk som hjälper dem om de behöver ställa en fråga snabbt om någonting.

MN: Känner ni att det finns några risker med sociala meder?

R2: Ja det är klart det finns risker. Det är uppenbart. Det märks snabbt att det kan slå ganska fel. Å andra sidan så hjälper inte policy i de fallen utan det enda som hjälper är ren nedstängning av access. Och kostnaden för det är så pass stor på andra håll att det inte är värt det.

MN: VI tittar även på malware och social engineering. Har ni några riktlinjer eller gått igenom vad man behöver göra för att undvika sådana situationer?

R2: Via vårt interna Yammer så har vi ganska snabb spridning om det är något på gång. I och med att de är säkerhetskonsulter så är de ju. det ingår i deras R2bb att hålla koll på vad som händer. Är det någon malware som sprids så går de snabbt ut, se upp för det här. Håll koll på de här sakerna. Internt sprids det väldigt snabbt.

MN: Er interna Yammer, vad är det för något.

R2: Yammer är som Facebook, fast inom bolag. Det är ett slutet nätverk. Man kopplar in alla anställda i det, sen får man en chatt klient. Men det är inte en till en utan många till många. Så man skriver in ett meddelande, alla kan skriva i det och svara tillbaka. Som ett forum men mycket, mycket snabbare. En mashup av facebook och Twitter inom bolag. Det används ganska vanligt inom bolag som ett sätt att snabbt få upp information. Det är inte publikt alls utan det är stängt inom bolagen.

MN: Gör ni någon kontroll av er närvaro på sociala medier, om den informationen som sprids om er organisation?

R2: Nej det skulle jag inte säga att vi gör.

MN: Väger nyttan med sociala nätverk upp riskerna?

R2: Ja det skulle jag definitivt säga. Effektiviten hos de som R2bbar här den ökar markant. Det är klart att det finns en risk med det, men dels att folk kan hålla kontakt med varandra och dels hela kunskapsutbytet. Det är en enorm kunskapskälla.

MN: Använder ni andra former av sociala medier för kunskapsutbyte, som wikis eller bloggar.

R2: Vi har använt internt wikis och bloggar men det är sällan det blir någon livskraft i det. Vi R2bbar så mycket med publika verktyg som möjligt. Vi har ett antal personer här som bloggar själva och de ser ju till att föra ut via vår hemsida så att gör de inlägg så kommer det att pushas ut på vår startsida direkt. Så vi försöker ju lyfta fram vad folk gör på den vägen. Men eftersom det är så mycket specialkompetenser så förlitar vi oss på att de pushar ut det och vi får ut det vi kan.

MN: Märker ni att ni gör skillnad på olika kunder beträffande säkerhetshanteringen, ställer kunder olika krav?

R2: Ja det är klart de gör. Vissa kunder ställer väldigt höga krav, andra ställer lite lägre krav.

RH: Hur fungerar det om ni ska gå med en ny kund?

R2: De kommer med ett NDA, ett kontrakt som säger att de här rättigheterna måste ni hålla er efter, det här gäller kring vår säkerhet, ni har inte rätt att säga någonting till en utomstående part, får ni material ska ni hantera det så här.

RH: Så det betyder att de konsulter som sitter på den verksamheten har samma privilegier och åtagande som de som sitter internt på den organisationen?

R2: Oftast har konsulten högre ansvar i och med att man kommer som extern part. Det kan vara att man inte får ta ut papper från verksamheten, man får inte prata om saker, man får inte dela ut saker. Det är oftast ganska höga krav. Det kan också stå i NDA:n att papper måste förvaras inlåsta om vi har dem här.

RH: Det här med VPN, är det något som ni ser som väldigt betryggande för att skicka och hämta information.

R2: Ja det skulle jag säga. Vi har ett ganska nedlåst VPN så vi har inte access överallt. Så det är ju egentligen tvåvägsskydd, så om man kommer in så kommer man inte hur långt som helst ändå.

Transkribering R3

RH: Vad har du för befattning?

R3: Jag är IT-chef för koncernen.

RH: Om du skulle beskriva verksamheten?

R3: Vi är en datalagringsintegratör, så det vi håller på med kortfattat är försäljning av datalagringsutrustning och tjänster runt omkring det.

RH: Hur stor är organisationen ungefär?

R3: Vi är dryga 600, finns i 13 länder, har 27 lokalkontor.

RH: Vad har (…) för syn på användning av sociala nätverk inom organisationen?

R3: Vi säger så att synen på sociala nätverk är positiv. Vi använder oss också av det i vår affär, kanske inte till 100 procent, men de används för att göra reklam och för att sprida information till våra kunder.

RH: kan man säga att det används för vardagligt arbete inom organisationen?

R3: Det kan man säga.

RH: Är det några särskilt utvalda som sitter ansvariga?

R3: Ja, framförallt är det de som jobbar med marketing eller försäljning som använder det.

RH: Har ni något problem som uppstått genom användning av sociala medier, främst ur ett tekniskt perspektiv snarare än ur ett PR-perspektiv.

R3: Ur något tekniskt perspektiv kan jag inte direkt påminna mig om att vi har haft. Men vi har haft ett problem för några år sen då det drevs en social kampanj mot våra anställda. Och då gjorde vi som så här för att försöka få någon pli på det hela, att problemet var ju att det var anonymt också. Så då tog vi reda på vilka det var som hade möjlighet att förse sig med den informationen och på så sätt kunde vi reda ut det. Sen tog vi kontakt med dessa personer så vi fick reda på var de var anställda. Så pratade vi med deras aviserare och sa till dem att det var dags att håller i era för annars så hjälper vi er med det.

RH: Har ni någon slags utbildning eller träning för era anställda beträffande sociala nätverk?

R3: Jag skulle säga att vi inte har det generellt. Utan det är för de som jobbar med det mer. Alltså mer marketing-människorna, de har fått utbildning i det. Men detta har inte gemeneman fått.

RH: Hur säkerställer ni hantering av andra företags data och information?

R3: I dagens läge så är det ganska enkelt så tillvida att om vi lagrar en kunds data så är det vår uppgift att se till att den är säkrad där. Och det innebär att den ska kunna vara konsistent 7/24

eller vad vi nu har för uppgifter på den. Men läsbar är inte denna typ av data för oss när man lagrar den. För då måste vi i sådana fall ha läs-access och det har vi inte. Utan vi bara lagrar datat, allting går men, så det är ingenting som man gör så bara att man kopplar inte en TP-kabel och går in och läser. Ofta regleras det via det avtalet man har upprättat med kunden också beroende på hur hög säkerhet de har på sin förvarade data, för vi har ju allt ifrån statliga myndigheter och vad det innebär till att vi har kommun och landsting plus ett antal vanliga företag men med en väldigt hög säkerhetsklassning och det regleras däri hur man ska handskas med det.

RH: Då är det alltså kundernas krav som bestämmer vad ni förhåller er till?

R3: Japp

RH: Har ni en säkerhetspolicy för IT överlag?

R3: Den reglerar vad det är som är tillåtet. Jag tror inte att det står något om vad som är förbjudet. Däremot så är den väldigt generellt skriven. Den är ungefär sex år gammal så det håller på och omarbetas nu för att hänga med litegrann. Den är täcker en hel del faktiskt.

RH: Innehåller den konsekvenser för vad som händer om man handlar på ett visst sätt?

R3: Det finns en sträcksats som säger det att om det är någon som bryter någon av de så kallade föreskrifterna, så kan det medföra att man kan få sparken om man gör det.

RH: Har ni en del i policyn som är riktad mot sociala medier eller är den mer allmän?

R3: Säkerhetspolicyn i sin tur, den är ett generellt ramverk där det finns ett antal sträcksatser, men den i sin tur hänvisar till en policy för social media.

RH: Hur skapades den? Var det av ledning, koncernnivå?

R3: Det är koncernnivå som har gjort det.

RH: så det är en speciell del i er säkerhetspolicy som behandlar sociala medier?

R3: I det stora paraplyträdet så ingår det här i informationssäkerhetspolicyn.

RH: Vem inom organisationen ansvarar för uppdatering och implementering av policyn?

R3: Det är jag som har ansvaret för att hålla den uppdaterad.

RH: Sitter du även på hantering kring sociala medier?

R3: Det var tidigare en som var ansvarig för kommunikation, men jag vet inte riktigt vem som har fått det uppdraget idag. Det kommer nog landa på mig iaf misstänker jag, om jag skulle ställa fråga uppåt till koncernchefen.

RH: Tror du att era säkerhetspolicyer kommer ändras eller påverkas allt eftersom sociala nätverk bli alltmer vanligt och populärt?

R3: ja det är jag ganska övertygad om för att jag håller redan nu på och skriver om den. Det är ett levande dokument det måste ju följa med. Riktlinjer och policy styr människor till viss del men människans beteende måste man ju ändå ta hänsyn till.

RH: Har ni speciella riktlinjer för hur anställda får använda sociala nätverk om man kollar på BYOD, företagets datorer, företagets mobiler?

R3: Den där frågan har vi faktiskt suttit och diskutera hur vi ska göra med för det som är problemet är ju att när man har en BYOD-produkt så är det ju så att om du ansluter den till företagets nätverk så måste du följa företagets policyer som ligger kring det där. Och då är den likställd med en egen dator, men det som är problemet är att vi inte lagligt riktigt helt koll på vad det är som gäller där. För att göra det måste man se till att de anställda skriver på vissa typer av policyer och sen ska man ha kontroll på det där. Det är så mycket runt omkring det där. Min förhoppning är att en BYOD den ska gälla likadant för alla om den är uppkopplad på företagets nätverk som det gäller för en företags-PC eller företagets mobila enheter, eller vad det nu kan vara.

[Mailad i efterhand, skriftligt svar]: Kommer det finnas speciella riktlinjer om man ser till malware, virus eller social engineering?

R3: Under intervjun nämnde du att ni hade en del av er policy som hanterade åtgärder för effekterna av malware, virus eller social engineering. Vi har några följdfrågor på detta som du gärna får hjälpa oss med.

[Mailad i efterhand, skriftligt svar]: Hur ser dessa åtgärder ut? Känner du att denna del av policyn är något som behöver uppdateras eller hanteras riskerna på ett bra sätt med dessa åtgärder? Hur håller ni er uppdaterade om vilka risker som är aktuella?

R3: Det finns faktiskt en täckning av det idag över policyn och hur man använder sociala medier. Så jag vet inte om det behöver kompletteras med någonting, men hoten blir ju helt annorlunda idag så vi får väl titta över den delen om vi behöver förstärka språkbruket i den just den policyn.

RH: Hur kontrollerar ni att policyn efterföljs?

R3: Hur en policy efterföljs brukar alltid slå igenom av sig själv. Det är alltid någon som ser att det är någonting eller någon som inte följer policyn, så då blir det ju att man får ta upp den i varje enskilt fall. Sen har vi vissa system som håller lite koll på hur man beter sig på internet, om man säger så.

RH: Tycker du att nyttan väger upp riskerna som finns?

R3: Ja det skulle jag vilja säga.

RH: Märker ni eller gör ni någon skillnad på olika kunder beträffande säkerhethantering?

R3: Ja, det gör vi.

Transkribering R4

MN: Vilken befattning har du?

R4: Jag är IT-Chef för Sigma

MN: Vad innebär det, vad är dina arbetsuppgifter?

R4: Jag är IT-ansvarig och IT-säkerhetsansvarig. Så jag ansvarar för Sigmas interna IT-stöd ut emot vår organisation och alla våra användare. Jag ser till att vi har systemstöd för att kunna jobba. Och ansvarar för vår policy när det gäller IT-policy och egentligen allt som har med IT att göra. Det kan vara grön-IT policy till exempel, som är vår miljö policy. Har även IT-säkerhetsansvaret.

MN: Så du arbetar inte så mycket mot kund utan mer in mot organisationen?

R4: Ja precis

MN: Hur skulle du kort beskriva verksamheten?

R4: Vi är ett IT-konsult företag som funnits i 15 år nu ungefär. Vi finns på 22 orter främst men har även en liten verksamhet utomlands. Det är i Kina och Ukraina främst men vi har även ett litet kontor i Finland och UK. Vi nischar in oss på systemutveckling och management konsulting. Det betyder alltså systemutveckling och åtagande har blivit en allt viktigare affär för oss, det vill säga att kunder vänder sig till Sigma för att få hjälp med att drifta, förvalta och utveckla system och applikationer. Våra största kunder är Volvo IT, Telia Sonera, Astra Seneca och IKEA. Så vi jobbar mest med stora företag men även med mellanstora företag som Lekolar och G4S och andra kunder som inte är så stora.

MN: Så då har ni konsulter som jobbar på Sigmas kontor men även konsulter som sitter ute hos kund?

R4: Ja och då är majoriteten de som sitter ute hos kund. Det svarar för ungefär 80 procent. De resterande 20 procenten är in house uppdrag, alltså kunduppdrag som vi utför i våra egna lokaler, som blir billigare både för oss och för kunden.

MN: Vad är Sigmas syn på externa sociala nätverk, som Facebook, Twitter och LinkedIn?

R4: Det är en fråga som inte är helt enkel att svara på. Fenomenet är ju relativt nytt och från början så hade jag personligen en uppfattning att det var främst konsumentprodukter, alltså att man använder det främst i privata sammanhang. Sen allt eftersom tiden har gått har vi fått inse att frågan är mer komplicerad än så därför att företag omnämns på nätet och i sociala sammanhang och då vill vi finnas där. Men jag kan ärligt säga att det inte är vår främsta kanal för att profilera oss. Vi finns där mest för att alla andra finns där. Om jag nu bara pratar om Facebook primärt. När det gäller LinkedIn och Twitter så är det mer privat, det är ju konto som man inte har som företag utan det är mer privat karaktär på de sociala medierna.

MN: Används sociala nätverk inom organisationen av anställda för någon slags kollaborations, kommunikations eller kunskapdsdelningsverktyg?

R4: Ja vi har börjat titta på att använda Yammer. Det är en företagsversion av Facebook. Så det har vi börjat titta på lite, vi har vissa enheter inom Sigma som använder det men det är ingen officiell kommunikationskanal utan ett fenomen som poppat upp för att det är trevligt och bra och underlättar kommunikationen för de som sitter ute på uppdrag. De som inte har kontakt med varandra på fikapauserna, så som vi kan göra som sitter internt.

MN: Så användande av sociala nätverk är framförallt använt ur PR synpunkt och sen främst för privat bruk av de anställda?

R4: Ja, precis

MN: Har det någon gång uppstått problem på grund av anställdas använda av sociala medier.

R4: Inte hittills

MN: Och ni känner inga effektivitetsproblem?

R4: Nej, det är svårt att mäta men det kan jag inte säga att vi gjort.

MN: Har ni utbildning eller träning av anställda gällande sociala medier?

R4: Nej det har vi inte. Men vi har tagit fram en policy för sociala medier, så om man kan anse det som utbildning så ok. Det är ett dokument på en A4 sida ungefär, där det står lite grann om hur vi ska förhålla oss till det som medarbetare inom Sigma. Så i den mån så kan vi säga att vi tagit fram en utbildning men det är inget som är...

MN: Men då är det något man får som nyanställd att läsa igenom och skriva på att man förstått?

R4: Ja precis.

MN: Hur skapades den eller vem är ansvarig för den, är det på ledningsnivå, genom överenskommelse mellan anställda eller finns det något ramverk som ligger bakom det?

R4: Det är faktiskt en tjej som är kommunikations och varumärkesansvarig. Hon sitter i Örebro och det är hon som skrivit policyn. Jag anser primärt inte att det är en IT fråga utan det är en varumärkesfråga, hur vi ska profilera Sigma och framförallt hur vi inte ska profilera Sigma. Så därför har hon fått det på sitt bord att skriva den.

MN: Och då är hon även med och implementerar och pushar ut den?

R4: Just det, precis.

MN: Finns det några speciella riktlinjer för hur man ska använda det gällande BYOD enheter, företagets datorer eller andra mobila enheter?

R4: Nej vi har ingen sådan policy med BYOD än så länge. Men det kommer säkert för frågan blir mer och mer spridd så det kommer säkert en sådan policy här inom kort.

MN: Finns det riktlinjer i den policyn vad som bör göras vid hot av till exempel malware eller social engineering?

R4: I vår IT policy har vi det.

MN: Får jag fråga vad den tar upp?

R4: Ja det får du men frågan är om jag kan svara på det rakt upp och ner. Det finns kapitel som talar om att dels så ska man ha antivirus på sina maskiner och vilket antivirus man ska ha. Och vad man ska göra om man misstänker att man fått in virus eller malware på sin maskin och hur man ska agera då. Det finns beskrivet där. I princip handlar det om att man ska anmäla det till mig eller någon support.

MN: Känner ni att det är ett problem, är det något som kommit upp med fler riktade eller generalla attacker?

R4: Nej det tycker jag inte.

MN: Ni har inte känt av några ökade risker med sociala medier?

R4: Nej det tycker jag inte, utan det ser ut som det gjort alltid.

MN: Hur kontrollerar ni att er policy för sociala medier efterföljs, gör ni någon slags check av er närvaro på sociala medier eller av anställdas användande?

R4: Nej jag tror faktiskt inte att vi gör det. Däremot är vi vaksamma om vi skulle få in rapporter om det skulle ske något oegentligheter eller så. Men det är inte det att vi aktivt sitter och kontrollerar sociala medier och vad folk skriver, det gör vi inte.

MN: Men ni har i er policy följder vad som händer om man inte följer den på ett riktigt sätt?

R4: Ja, det har vi.

MN: Väger nyttan med sociala nätverk upp riskerna?

R4: Det var en bra fråga. Jag ser egentligen inte nyttan med sociala nätverk på samma sätt som de flesta andra gör verkar det som. Jag ser sociala nätverk som något mer privat. För Sigmas del så har det inte gett så mycket nytta egentligen, utan vi finns på sociala medier för att de andra finns där. Vi använder inte sociala medier som en säljkanal. Våra kunder finns inte på sociala medier på det sättet. Det är klart att många finns där men då är det som privat. Det är en jättesvår fråga.

MN: Eftersom ni sitter på mycket information som tillhör era kunder, hur säkerställer ni hanteringen av era kunders data och information?

R4: Ja det gör i princip kunderna själva därför att får vi in uppdrag från en kund som har väldigt höga säkerhetskrav vilket de flesta har, då får vi i regel alltid utrustning från kunden, det vill säga en dator och VPN ingång. Då jobbar man rakt in i kundens miljö med kundens utrustning. Så därför blir det kundens ramverk och krav som styr åtkomst och säkerhetsnivåer. Och det skiljer ju från kund till kund, så en kund är inte den andra lik utan det är väldigt stor

skillnad beroende på vem man har att göra med. Astra Seneca till exempel har ju enorma krav på sin IT säkerhet medan andra kunder inte har lika höga krav.

MN: Är ni tvungna att följa kunder policyer?

R4: Ja, det måste vi göra.

Referenser

Artiklar

Aula, P., (2010). *"Social media, reputation risk and ambient publicity management"*, Strategy & Leadership, vol. 38 no. 6 2010, pp. 43-49

Allen, M., (2009), *"Tim O'Reilly and Web 2.0: The economics of memetic liberty and Control"*, Communication, Politics and Culture, 42:2, pp. 6 – 23.

Bakhshi, T., Papadaki, M., Furnell, S., (2009), *"Social engineering: assessing vulnerabilities in practice"*, Information Management & Computer Security, Vol. 17 Iss: 1, pp. 53 – 63.

Brody, G. R., Brizzee B. W., Cano, L., (2012), *"Flying under the radar: social engineering"*, International Journal of Accounting and Information Management, Vol. 20 Iss: 4 pp. 335 – 347.

Cain, A., (2012), *"The social media scene"*. Internal Auditor [serial online]. August 2012;69(4), pp. 44-49. Available from: Business Source Complete, Ipswich, MA.

Carminati, B., Ferrari, E., (2008), *"Access control and privacy in web-based social networks"*, International Journal of Web Information Systems, Vol. 4 Iss: 4 pp. 395 – 415.

Dodge, R.C., Carver, C., Ferguson, A.J., (2007), *"Phishing for user security awareness"*, Computers & Security, Vol. 26, pp. 73 – 80.

Field, J., Chelliah, J., (2012), *"Social-media misuse a ticking time-bomb for employers: Robust policies and procedures needed to reduce the risks"*, Human Resource Management International Digest, Vol. 20 Iss: 7 pp. 36 – 38.

Garrigos-Simon, F.J., Alcamí, R.L., Ribera, T.B., (2012), *"Social networks and Web 3.0: their impact on the management and marketing of organizations"*, Management Decision, Vol. 50 Iss: 10, pp. 1880 – 1890.

Gatewood, B., (2012), *"The nuts and bolts of making BYOD work"*. Information Management Journal, 46(6), pp. 26 – 30.

Hasan, M., Prajapati, N., Vohara, S., (2010), *"Case study on social engineering techniques for persuation"*, International journal on applications of graph theory in wireless ad hoc networks and sensor networks, (GRAPH-HOC) Vol.2, No.2, June 2010.

He, W., (2012), *"A review of social media security risks and mitigation techniques"*, Journal Of Systems And Information Technology, 14(2), pp. 171 – 180.

Hughes, L.A., DeLone, G. J., (2007), *"Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both?",* Social Science Computer Review 2007 25: 78.

Huy Q., Shipilov A., (2012), *"The Key to Social Media Success Within Organizations"*, Mit Sloan Management Review.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., Pu, C., (2011), *"Reverse Social Engineering Attacks in Online Social Networks"*, DMIVA 2011, LNCS 6739, pp. 55 – 74.

Kapsali, M., (2011), *"How to implement innovation policies through projects successfully"*, Technovation, Vol 31, Iss 12, December 2011, pp. 615 – 626.

Keenan, A., Shiri, A., (2009), *"Sociability and social interaction on social networking websites"*, Library Review, Vol. 58 Iss: 6 pp. 438 – 450.

Koch, H., Gonzalez, E., Leidner, D., (2012), *"Bridging the work/social divide: the emotional response to organizational social networking sites"*, European Journal of Information Systems (2012), pp. 1 – 19.

Karlsson, M., (2013, 7 februari). *Computer Sweden – Säkerhet, s. 19*

Kaplan, M. A., Haenlein, M., (2010), *"Users of the world, unite! The challenges and opportunities of Social Media",* Business Horizons, Vol. 53, Iss 1, January–February 2010, pp. 59 – 68.

Milošević, N., (2013), *"History of Malware"*, Computer History

Rudman, R. J., (2009), *"Incremental risks in Web 2.0 applications"*, The Electronic Library Vol. 28 No. 2, 2010, pp. 210 – 230.

Seale, C., (1999), *"The quality of qualitative reseach"*, Sage Publications Ltd.

Ubeda, J.E., Gieure, C., de-la-Cruz, C., Sastre, O., (2013), *"Communication in new technology based-firms"*, Management Decision, Vol. 51 Iss: 3, pp. 615 – 628.

Van Zyl A. (2008), *"The impact of Social Networking 2.0 on organisations"*, Electronic Library [serial online] November 13, 2009;27(6), pp. 906 – 918.

Witten, B., Nachenberg, C., (2005), *"Malware Evolution: A Snapshot of Threats and Countermeasures in 2005"*

Workman, M., (2008), *"A test of interventions for security threats from social engineering"*, Information Management & Computer Security, Vol. 16 Iss: 5, pp. 463 – 483.

Böcker

Bryman, A (2001). *Social Research Methods*. Oxford University Press, USA.

Dhillon, G. (2007). *Principles of information systems security*. Wiley.

Jacobsen, D.I. (2002). *Vad, hur och varför?* Lund: Studentlitteratur.

LeVeque, V. (2006). *Information Systems*, John Wiley & Sons Inc.

Schein, E.H. (2009): *The Corporate Culture Survival Guide*. Jossey-Bass.

Schött, K., Melin, L., Moberg, B., Strand, H. (2007): *Studentens skrivhandbok*. Stockholm: Liber AB.

Walliman N. (2006). *Social Research Methods*. SAGE Publications, Ltd.

Whitepapers

Dimensional Research, 2011, The Risk of Social Engineering on Information Security: A Survey of IT-Professionals. [Elektronisk]. Tillgänglig: http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf [2013-05-03].

Cisco Systems, 2008, Data leakage worldwide: the effectiveness of security policies. [Elektronisk]. Tillgänglig: www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.pdf [2013-04-09].

Clearswift, 2011, Worldwide clampdown on technology as businesses overreact to high profile data breaches. [Elektronisk]. Tillgänglig: http://www.clearswift.com/news/press-releases/worldwide-clampdown-on-technology-as-businesses-overreact-to-high-profile-data-breaches [2013-04-02].

IBM, 2007, Achieving tangible business benefits with social computing, [Elektronisk]. Tillgänglig: http://www-935.ibm.com/services/in/cio/pdf/empow_wp_business_benefits_of_social_computing.pdf [2013-04-08].

Ponemon Institute, 2011, Global Survey on Social Media Risks, [Elektronisk]. Tillgänglig: https://www.websense.com/assets/reports/websense-social-media-ponemon-report.pdf [2013-02-15].

SilkRoad, 2012, Social Media & Workplace Collaboration http://pages.silkroad.com/rs/silkroad/images/Social-Media-Workplace-Collaboration-SilkRoad-TalentTalk-Report.pdf [2013-03-06].

Internetreferenser

Bullguard. Malware - definition, history and classification, [Elektronisk]. Tillgänglig: http://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification.aspx. [2013-04-02].

Checkfacebook, [Elektronisk]. Tillgänglig: http://www.checkfacebook.com/. [2013-04-03].

Cisco, 2012, Cisco Social Media Policy [Elektronisk] Tillgänglig: http://www.scribd.com/doc/33461366/Cisco-Social-Media-Policy-Guidelines-and-FAQs. [2013-04-03].

Cormode, G., Key differances between Web 1.0 and Web 2.0, [Elektronisk]. First Monday. Tillgänglig: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2125/1972. [2013-04-03].

Dell, 2011, Global Social Media Policy [Elektronisk], Tillgänglig: http://www.dell.com/Learn/us/en/uscorp1/corp-comm/social-media-policy?c=us&l=en&s=corp&delphi:gr=true. [2013-04-03].

Fair Work Australia, 2011, Glen Stutsel v Linfox Australia Pty Ltd [Elektronisk] http://www.fwc.gov.au/decisionssigned/html/2011fwa8444.htm. [2013-04-11].

Gartner, 2012, Gartner IT Glossary [Elektronisk] Tillgänglig: http://www.gartner.com/it-glossary/. [2013-04-09].

Intel, Intel Social Media Guidelines [Elektronisk] Tillgänglig: http://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html. [2013-04-02].

Lowensohn, J, Apple: Employee computers were targeted in hack attack, [Elektronisk]. CNet, 2013-02-19. TIllgänglig: http://news.cnet.com/8301-1009_3-57570096-83/apple-employee-computers-were-targeted-in-hack-attack/. [2013-03-28].

Maness, M. J, Library 2.0 Theory: Web 2.0 and Its Implications for Libraries [Elektronisk]. Tillgänglig: http://www.webology.org/2006/v3n2/a25.html. [2013-04-08].

Nielsen, Global Audience Spends Two Hours More a Month on Social Networks than Last Year [Elektronisk]. Tillgänglig: http://www.nielsen.com/us/en/newswire/2010/global-audience-spends-two-hours-more-a-month-on-social-networks-than-last-year.html. [2013-05-14].

Norton, Crimeware: Trojans & Spyware. [Elektronisk]. Tillgänglig: http://us.norton.com/cybercrime-trojansspyware/promo. [2013-05-03].

PewResearch 2013, Pew Internet: Social Networking (full detail) [Elektronisk]. Tillgänglig: http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx. [2013-04-08].

Rundkvist, F. (2012). Sofia, 22, blåstes av nya nätbluffen. [Elektronisk]. Aftonbladet. Tillgänglig: http://www.aftonbladet.se/nyheter/article14578574.ab. [2013-04-05].

Socialbakers, Facebook Statistics by Country, [Elektronisk]. Tillgänglig: http://www.socialbakers.com/facebook-statistics/. [2013-04-03].

Symantec, 2012, Internet security threat report. [Elektronisk]. Tillgänglig: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf [2013-04-04].

Yammer, 2013, [Elektronisk]. Tillgänglig: https://www.yammer.com/product/. [2013-05-15].

Föreläsningsmaterial

Bergh, I. & Johannesson, K. (senast uppdaterad 2012-06-21). Referenshantering. [Elektronisk]. Högskolan i Skövde. Tillgänglig: http://www.his.se/Documents/biblioteket/Referenshantering_kj.pdf. [2012-06-26].