EKONOMIHÖGSKOLAN
Lunds universitet

De största hoten mot ett företags informationssystem

Kandidatuppsats, 15 högskolepoäng, INFK03 i informatik

Framlagd: 2011-01-12

Författare: Niclas Månsson

Handledare: Anders Svensson
Examinatorer: Hans Lundin, Claus Persson

Titel: De största hoten mot ett företags informationssystem
Författare: Niclas Månsson
Utgivare: Institutionen för informatik
Handledare: Anders Svensson
Examinatorer: Hans Lundin, Claus Persson
Publiceringsår: 2011
Uppsatstyp: Kandidatuppsats
Språk: Svenska
Nyckelord: Informationssäkerhet, Hot, Malware, Insider, Social engineering, Mobila enheter

Abstrakt

Information är en viktig resurs för företag och oavsett hur de bedriver verksamheten så ställs det krav på informationssäkerhet. Syftet med denna uppsats är att få kunskap om vilka de största hoten är mot ett företags informationssystem. I den teoretiska genomgången tas hot som malware, insiders, Social engineering, olyckor och misstag samt risker och hot med mobila enheter upp. Resultaten av undersökningen som genomfördes med frågeformulär visar att de största hoten är främst malware hot, speciellt virus samt misstags och olycksrelaterade hot. Samtliga företag som deltog i studien hade virus på deras topp fem listor över hot mot deras informationssystem. Detta visar precis som i litteraturen att det är det vanligaste förekommande hotet. För att skydda sig mot hoten krävs det åtgärder som antivirusprogram, brandväggar, loggning över nättrafik, backup och att alla program hålls uppdaterade. Hot som Malware orsakas oftast av attackerare som har orsak att skada något eller någon men det behövs någon som för in det i företagets system t.ex. att någon anställd gör något misstag. Det kan bli stora konsekvenser för företaget om hoten utlöses. Det är därför viktigt att företagen gör en analys av säkerhetsriskerna regelbundet.

Innehållsförteckning

1. Inledning

1.1. Bakgrund

Information och kunskapsöverföring har förändrats över tiden från tal, handling och skrift till dagens Internetanvändning. Internet som det ser ut idag har inte så lång historia utan startade 1994 (Carlsson, 2007). Det fanns dock motsvarande äldre versioner som har använts inom det militära (ARPANET) och inom Universitetsvärlden (SUNET) (Carlsson, 2007). Idag finns det mångdubblade möjligheter att överföra information mellan företag och personer. Många människor använder Internet för e-mail, e-handel, söka information, informera och en mängd andra funktioner dagligen.

I dagens olika verksamhetsområden kommunicerar och interagerar personer genom informationssystem. Informationssystemet stödjer kommunikationen och handlandet i verksamheten (Lagersten, 2009).

Företag kan med ett väl uppbyggt informationssystem på ett snabbt och enkelt sätt informera, kommunicera och söka information vilket medför förenkling av många arbetsuppgifter. Det mesta ser mycket positivt ut men det finns dock en negativ sida och det är hoten mot informationssystemen.

I media förekommer allt oftare artiklar och inslag om olika hot mot informationssystem. Maskattacker mot mobiltelefoner, förgiftade sökresultat och skadlig kod i annonser för att nämna några av de 13 allvarligaste hot mot IT-säkerheten som vi kan få problem med under 2010 enligt Jenny Stadgis (2010). Den 21 april 2010 publicerade metroteknik följande ”IT-attackerna är fler än någonsin” och ”Största hoten mot företagen”. De största hoten som angavs var riktade attacker som specialskrivna trojaner, maskar som vandrar runt och tar över datorer, gårdagens teknik som används och en övertro till tekniken (Örnborg & Jacobsen, 2010).

Seminarier är ett annat forum som tar upp IT-säkerhet. Ett exempel är Sentors seminarium den 28 maj 2009 där Marcus Nohlberg, doktor i informationssäkerhet föreläste under rubriken ”Social engineering är det största hotet mot din verksamhet”. Det finns många olika hot men vilka anses som de största hoten för ett företag?

Hot mot informationssystem är ingen nyhet utan har funnits innan det kommersiella Internet. Redan 1981 spreds det första viruset Elk Cloner via Apple II datorernas floppydisk (Carlsson, 2007).

Många företag är beroende av att ha fungerande IT. Om hoten mot informationssystemen blir genomförda så får det stora konsekvenser för företagen. Står datorerna stilla påverkar det hela företaget speciellt om IT-driftstoppet blir långvarigt (Myhr et al, 2004). Kan inte arbetet genomföras blir konsekvensen att det ger stora ekonomiska förluster för företagen.
För att identifiera de hot som kan uppstå är det viktigt att göra en risk- och konsekvensanalys samt göra en bedömning av vad som kan hända med verksamheten om hoten genomförs

(Syrén, 2005). Att utarbeta en åtgärdsplan ger möjlighet till att förbättra informationssäkerheten och bedöma vilka säkerhetsrutiner och skydd som det finns behov av samt i vilken omfattning.

Genom att undersöka vilka de största hoten och säkerhetsriskerna är, går det att utarbeta rutiner och lösningar för att minska säkerhetsriskerna. Detta gör denna studie intressant och viktig.

1.2. Problemformulering

Datorn är vårt vanligaste arbetsredskap och enligt Arbetsmiljöverket (2010) så använder nästan 70 % av de yrkesarbetande en dator någon gång under arbetsdagen. Informationsteknologi (IT) används allt mer för att underlätta arbetet. Beroendet av IT-stöd ökar i och med att fler och fler tjänster erbjuds över Internet. Det innebär att företagen förlitar sig på att de IT-baserade systemen skall fungera och det är en förutsättning för att arbetsuppgifterna skall kunna göras effektivt. Region Skåne (2010) anser att det nästan inte finns några verksamheter idag som klarar IT-störningar eller avbrott utan att de ger konsekvenser för företaget/organisationen.

Information är en viktig resurs för företaget och oavsett hur de bedriver verksamheten så ställs det krav på säker informationshantering. Det innebär att all information i ett företag eller organisation använder i verksamheten måste skyddas (Lundblad, 2005; Syrén, 2005). Därför måste företaget eller organisationen arbeta med informationssäkerhet och vidta sådana åtgärder att företaget känner sig säkert (Syrén, 2005). Men vad måste informationssystemen skyddas emot? Vilka är de största och mest frekventa hoten? De verksamhetsansvariga måste göra en riskanalys dvs. systematiskt identifiera vilka hot de kan utsättas för (Syrén, 2005). Region Skåne (2010) anser att det är viktigt med en klar bild över vilka hot som är relevanta för verksamheten för att kunna bedöma hur sannolikt det är att hoten kommer att utlösas. Även Syrén (2005) anser att alla företag såväl små som stora bör genomföra en analys för att se hotbilden. Därför bör det undersökas vilka de största hoten är som kan ingå i en hotbild mot ett företags informationssystem och om det finns skillnader i hotbild mellan företag som har olika verksamheter. Dessutom bör det göras bedömningar om det finns skillnader mellan företagens analyser och säkerhetsanalytikers expertråd.

1.3. Forskningsfråga

I denna uppsats ämnas följande fråga och underfrågor att besvaras:

- Vilka är de största hoten mot ett företags informationssystem?
    - Vilken skada kan hoten göra om de utlöses?
    - Hur kan företaget skydda sig mot hoten?
    - Vem eller vad kan vara orsak till hoten?

1.4. Syfte

Syftet med studien är att identifiera och få kunskap om vilka de största hoten är mot ett företags informationssystem. Denna kunskap kan sedan företag/organisation använda när de gör riskanalys. Målgruppen för studien är personer som arbetar med informationssäkerhet samt personer som söker kunskap inom området informationssäkerhet eller informatiker, IT-specialister, IT-ansvariga som är intresserade av ämnet.

1.5. Avgränsningar

Informationssystem kan beskrivas som ett system som med IT-stöd där information samlas in, lagras och bearbetas samt distribueras. Undersökningen inriktade sig på de fem största hoten som ett företag ställs emot när det gäller informationssäkerhet då det skulle ha blivit för omfattande arbete att ta med alla hot. Det har inte varit möjligt att ha med alla företag/organisationer i undersökningen utan ett urval gjordes. Det har inte heller varit möjligt att inrikta undersökningen mot en specifik bransch.

2. Litteraturgenomgång

2.1. Informationssäkerhet

Information har utvecklats från att vara en abstrakt tillgång till att vara en definierbar, mätbar och skyddsvärd tillgång. Därför måste företag vidta åtgärder för att skydda sin information mot otillåten åtkomst, förändring eller förfalskning. Det går att upptäcka och registrera identifierade hot om företaget har vidtagit skyddsåtgärder (Syrén, 2005). Men vad är ett hot? Enligt Gollmann (2006) är ett hot när någon/något utför en handling för att utnyttja sårbarheter för att skada någons tillgångar. För att skydda sina tillgångar är skyddsåtgärder viktiga. Skyddsåtgärderna innebär även att riskerna minskar för att hot skall utlösas. Informationssäkerhet innefattar hela infrastrukturen i ett företag. Därför är informationssäkerhet en väldigt viktig del av företagets riskhantering (Syrén, 2005).

Informationssäkerhet är något experter ofta talar om, men vad innebär det egentligen. Vilken information är det som ska säkras? Det många tror är att det är hemlig information som ska säkras. Men egentligen är det all den information som ett företag använder som kan vara intressant att skydda. Något som alltid har varit centralt i alla typer av verksamheter är just information. Nu för tiden är information inte bara viktig utan den är en förutsättning för att verksamheten ska kunna fortsätta. Ett exempel på det är att om en tidnings informationssystem skulle gå ner kan verksamheten inte fungera alls. Det finns nästan inga verksamheter som klarar sig helt utan ett informationssystem. Därför har skydd av information kommit att hamna i centrum. Om det inte finns ett bra skydd av informationen saknar företaget/organisationen även ett skydd för verksamheten i sin helhet. (Lundblad, 2005)

2.2. Malware

Ordet malware är en förkortning på malicious software och kan även kallas för malicious code. De olika typerna av malware är klassificerade utefter hur de sprider sig, med ett fåtal undantag (Ahmad et al, 2002). Malware är en programvara som har för avsikt att skada. Denna typ av hot har funnits under många år men har ökat i farlighet under årens lopp på grund av Internet. Innan Internet fanns var det tvunget att fysiskt transportera programvaran till datorn. Programvaran fanns t.ex. på en diskett som sedan en användare använde och utan vetskap om det fick användaren in skadlig programvara i datorn. Begränsning med att behöva vara i fysisk kontakt har försvunnit i och med Internet. Nu går det enkelt att hitta sårbarheter via nätet eller så går det att bifoga programvaran i ett e-mail som är ett enkelt sätt att sprida det på (Dubrawsky, 2007).

2.2.1. Virus

Den mest klassiska typen av malware är virus som är ett vanligt förekommande hot och är även det som nämns oftast i media samt i folkmun när det gäller malware hot. Men det händer dock att media och personer som inte har någon större kunskap om datorer misstar andra malware hot för virus när de i själva verket är något annat (Pfleeger & Pfleeger, 2003). Ett datavirus brukar definieras som ett självreplikerande datorprogram som stör en dators hårdvara, mjukvara eller operativsystem (Ahmad, 2002). Virus är utformade för att kopiera och för att undankomma att bli upptäckta. Virus måste precis som andra datorprogram exekveras för att fungera samt att datorn måste följa virusets instruktioner. Dessa instruktioner är själva nyttolasten av viruset. Den kan störa eller ändra datafiler, visa meddelande eller få operativsystemet att sluta fungera (Dubrawsky, 2007).

Virus sprids när dess instruktioner som kör program skickas från en dator till en annan. Ett virus kan kopiera sig själv till disketter, hårddiskar, datorprogram, längs det lokala nätverket och genom Internet. Men för att nätverket är infekterat med ett virus eller att det laddats ner programvara som innehåller ett virus behöver det inte betyda att datorn blir infekterad. Det är själva koden som måste köras för att datorn ska bli infekterad. Men om datorn skulle drabbas av ett virus och det inte körs är det troligt att det lurar ens operativsystem till att köra det. Virus kan sätta sig på hederlig programvara och det kan hända när program skapas, öppnas eller modifieras. När användaren sedan kör programmet startas även viruset. (Dubrawsky, 2007)

Parasitic virus är den vanligaste formen av virus. Det viruset gör är att fästa sig på körbara filer och när filen sedan körs kopierar den sig till andra körbara filer som då infekteras (Stallings, 2003). Den ändrar inte själva ”host” filen utan den lägger till värden som gör att den startar viruset före själva filen (Dubrawsky, 2007).

Memory-resident virus är ett virus som sätter sig i resident koden i minnet. Denna kod används för att slippa ladda om program varje gång det behövs, istället lagras informationen i resident koden för att det snabbt ska gå att starta. Varje gång den koden körs, vilket är väldigt ofta på ett system, kommer även viruset att köras. När viruset körs letar det efter ställen att sprida sig till. Om det t.ex. kopplas in en portabel disk kan den då infektera den och på så sätt sprida sig vidare. (Pfleeger & Pfleeger, 2003)

Boot sector virus finns på den första delen av portionen av hårddisken som just kallas för boot sektorn, det gäller även disketter och cd-skivor. Detta virus ersätter antingen program som lagrar information om diskens innehåll eller program som startar datorn. Viruset körs när systemet bootar från den disk som blivit infekterad. Denna typ av virus sprids oftast via fysiska utbyten. (Dubrawsky, 2007)

Stealth virus är en typ av virus som har en speciell design för att kunna undgå att bli upptäckt av olika antivirusprogram. Ett exempel på hur ett stealth virus kan dölja sig är att det använder sig av komprimering så att när ett program infekteras blir det exakt samma längd som det icke-infekterade programmet. (Stallings, 2003)

Polymorphic virus är ett virus som kan ändra sitt utseende. Därav har det fått sitt namn, poly som betyder många och morph som betyder form (Pfleeger & Pfleeger, 2003). Det viruset gör är att mutera sig vid varje infektionstillfälle, vilket gör det nästintill omöjligt att upptäcka den

genom dess ”signatur”. En signatur är de strängar i ett virus som gör det möjligt att identifiera det. Detta använder bland annat antivirusprogram för att upptäcka virus (Stallings, 2003).

Den ideala lösningen på virushot är förebyggande medel. Det bästa är att helt enkelt aldrig få in ett virus i systemet till att börja med. Detta är dock nästintill omöjligt att lyckas med helt, men det kommer att minska antalet virus som tar sig igenom. Näst bästa tillvägagångssättet är att använda sig av detection, identification och removal. Det vill säga att upptäcka när något blivit infekterat och lokalisera var det befinner sig, för att sedan identifiera vilket specifikt virus det rör sig om. Därefter gäller det att ta bort viruset från alla infekterade system och alla dess spår så det inte kan sprida sig vidare (Stallings, 2003). För att undvika att få virus bör alla program sökas igenom med ett antivirusprogram innan de körs. Det gäller också att hålla sitt antivirusprogram uppdaterat för att det ska kunna upptäcka de senaste virusen (Ahmad et al, 2002).

2.2.2. Maskar

Maskar är en annan typ av malware som är väldigt likt ett virus bortsätt ifrån att den inte kan återskapa sig själv lokalt (Ahmad et al, 2002). En mask är ett självreplikerande program som vistas i det aktiva minnet och duplicerar sig själv med hjälp av ett datanätverk. Maskar körs automatiskt inom operativsystemet eller mjukvaran och de är inte synliga för användaren. En mask kan sprida sig på många olika sätt, genom e-mail, över Internet, via P2P (peer-to-peer) program för att nämna några. Maskar är osynliga för användaren som inte märker dem förrän alla resurserna för nätverket är använda eller att datorn är påverkad till den grad att den inte går att använda längre (Dubrawsky, 2007).

En aspekt av maskar som är intressant är att de kan bryta sig in i system via sårbarheter i mjukvara. Dessa maskar är en form av automatiska hackers som bryter sig in i system för att sedan leta runt för att kunna attackera ännu fler system. (Ahmad et al, 2002)

År 2003 kom den första ultrasnabba flash masken Slammer. Den infekterade hundratusentals datorer världen över och stängde av uttagsautomater samt påverkade Internets namnservrar. En annan känd mask som kom i maj 2004 var Sasser som infekterade statliga datorer och företags datorer, vilket bland annat ledde till att flyg och järnvägstrafiken tvingades stanna. (Leeuw, 2007)

Det finns en hel del saker som det går att göra för att skydda sig mot maskar. En sak som är viktig är utbildning av användare angående maskar för att förhindra att de drar in dem. Det går att förhindra många maskattacker då de flesta använder sig av kända sårbarheter och inte icke tidigare kända. Då de är kända är de möjliga att förhindra genom uppdatering av program med de nyaste patcharna som just tar bort dessa sårbarheter. Speciellt Microsofts program då de har en väldigt stor del av marknaden vilket innebär att hoten mot deras programvara är stor. Problemet är att oftast tar det ett tag innan de installeras pga. att de som kan inte har tid eller att de helt enkelt inte vet om att den släppts. Något som också är viktigt är att konfigurera sin brandvägg korrekt och bara låta nödvändiga portar vara öppna samt ha ett uppdaterat antivirusprogram. (Aycock, 2006)

2.2.3. Trojaner

En trojan är ganska lik ett virus men är en kategori för sig själv. Trojaner är kod som har förklätt sig till att vara godartade program men som sedan beter sig på ett oväntat och vanligtvis på ett skadligt sätt (Ahmad et al, 2002). En trojan är ett program med en gömd sidoeffekt som inte är specificerad i programmets dokumentation och användaren har inte för avsikt att köra det (Gollmann, 2006). En trojansk häst används på samma sätt som i Homeros Iliaden[1], där grekerna byggde en enorm trähäst som var ihålig och fyllde den med 30 man. Sedan lämnade de den på stranden och låtsades att segla iväg. Trojanerna släpade sedan denna häst in innanför stadens murar i tron att det var gudarnas vilja. På natten kröp sedan grekerna i hästen ut och slog ut vakterna samt öppnade porten till staden så att grekerna kunde storma staden. Vilket då ledde till att trojanerna blev besegrade. Men hästen är nu istället ett program som innehåller skadlig kod istället för människor. Det kan vara ett litet spel som ser helt ofarligt ut men i det döljer sig skadlig kod som körs. En trojan kan förstöra allt på en hårddisk om det vill sig illa. Men en sak som är bra, om man nu kan säga det om man får en trojan på datorn, är att den inte sprider sig från en dator till en annan (Dubrawsky, 2007).

Det finns flera olika sätt att bli utsatt för en trojan men ett vanligt sätt är att någon skickar ett e-mail med en bifogad fil som innehåller trojanen. När personen sedan kör programmet kommer trojanen att installera sig på systemet, men helt utan att användaren märker av det då det sker i bakgrunden av programmet. (Dubrawsky, 2007)

En begränsning som trojaner har är att användare måste acceptera eller köra trojanen för att bli utsatt för den. Användare måste alltså övertygas till att köra den. Därför brukar de få namn som är förtroendeingivande och att de döljer programmet i en förklädnad vilket gör att användare tror att det är något helt annat. Det kan ibland vara så enkelt att de bara byter namn på filen till ett namn som redan finns på ett känt program. Men det kan också vara ett helt program som ser ut att vara ett vanligt program när det körs. Ett exempel på en sådan trojan är Pokemon trojanen. Det den gjorde var att visa animerade bilder av pokemons på skärmen, men i bakgrunden skickade programmet e-mail till alla i användarens mail-lista och tog bort varenda fil i Windows directory. Användaren ser inte att programmet skickar e-mail och tar bort filer från systemet. (Ahmad et al, 2002)

Ett annat exempel på en trojan är QAZ som infekterade många datorer år 2000. Den spred sig inom nätverkets delade datasystem där den infekterade Notepad.exe filen. När systemet fick trojanen bytte den direkt namn på Notepad.exe till Note.com och skapade en virus infekterad fil med namnet Notepad.exe. Den gjorde även att filen kördes när systemet bootades upp. Det den sen gjorde var att öppna portar vilket medförde att hackare kunde ta sig in. Just den här trojanen användes bland annat till att hacka sig in i Microsofts nätverk. Det som gjorde den effektiv var att det hade sagts att alla textfiler var säkra från virus vilket ledde till att ingen tvekade att köra ett program som associeras med Notepad. Det som gör trojaner extra farliga är att de kan vara program för att fjärrstyra. De som använder trojanen till en fjärrstyrningsserver kan nu ansluta till din dator (Dubrawsky, 2007). Att försvara sig mot sådana här attacker är egentligen ganska enkelt. Det gäller att inte köra okända program som kanske inte är helt säkra. Detta har sagts under väldigt lång tid och de flesta följer det men det finns alltid något som människan är svag för. Det kanske är ett barn som dansar i en video som sprids runt på Internet och då är det garanterat en viss procent av människor som kommer att öppna denna för att titta. Under tiden de tittar på denna skickar programmet många

[1] Iliaden är en grekisk hjältedikt som innehåller 24 sånger och är gjord av Homeros på 700-talet fKr. Den tar upp grekernas belägring av Troja (Josephson, 2007).

spammail till alla användarens kontakter, tar bort filer och ändrar alla ens lösenord. När det hänt tycker den som utsatts för attacken förmodligen inte att videon var så trevlig längre (Ahmad et al, 2002).

Något som har gjort det mer förvirrande för människor att avgöra vad som är säkert att öppna och vad som inte är säkert är bland annat elektroniska gratulationskort. De skickar dessa kort till sina vänner och bekanta när de t.ex. fyller år. När deras vän skickar ett gratulationskort så tänker de direkt att det är säkert för de har ju fått kort av vännen innan och då har det inte hänt något. Men det de inte vet är att vännen har utsatts för en trojan och det är i själva verket den som skickar ut gratulationskortet som även den innehåller en trojan. (Ahmad et al, 2002)

2.2.4. Spyware

Spyware är ett växande hot mot dagens företag. Men när spyware först började dyka upp i företagens nätverk sågs det bara som ett elände och inte som ett hot mot hela företaget. Det rörde sig ofta om ett fåtal anställda som surfade på osäkra sidor på webben och därmed drog med sig spyware. På senare år har dock företagen börjat ta spyware på mer allvar när det gäller nätverkssäkerheten då de är en stor faktisk risk. (Baskin & Piltzecker, 2006)

Spyware har som funktion att spionera på de maskinerna den är installerad på. Det de gör är att samla in personlig information som de sedan kan använda av diverse anledningar. De flesta spyware är inte direkt skadliga utan det största problemet är att de förbrukar datorernas resurser. Då spyware är ganska vanligt har det lett till att flera anti-spyware program har utvecklats, Ad-Aware, Spyware Doctor och Malwarebytes Anti-Malware för att nämna några. (Dubrawsky, 2007)

Det finns naturligtvis flera olika syften med spyware. Det kan vara en del av marketing, att det visar reklam under tiden användaren surfar (adware), att användare flyttas till sidor som användaren egentligen inte hade för avsikt att besöka och framförallt då den kriminella avsikten som att stjäla åt sig lösenord eller kreditnummer (Dubrawsky, 2007). Spyware har utvecklats från att kunna rapportera om användarens webbhistorik till att kunna leta efter information i filsystemet på en dator, lagra tangentnedslag för att få tag i lösenord och liknande. Denna utveckling har ökat företagens oro för att få in spyware i deras system (Baskin & Piltzecker, 2006). När det gäller spyware luras användaren oftast till att ladda ner dem i samband med något annat verktyg eller att de utnyttjar brister i webbläsare (Dubrawsky, 2007).

När det gäller spridningen av spyware måste de oftast installeras på varje dator, den sprider sig inte själv. Då de oftast är relaterade till användarens surfaktiviteter kan de få datorn att visa enorma mängder med pop-up fönster. Men alla typer av spyware är inte bara till för att skada som sagt utan vissa används på ett bra sätt och är lagliga. Det de gör är t.ex. att hålla reda på betalning för program. (Dubrawsky, 2007)

En skrämmande aspekt angående spyware som kommit in i företagen är dess rena överflöd. Baskin & Piltzecker (2006) beskriver en undersökning där 96 % av företagen som tillfrågades tycker att deras brandvägg och antivirusprogram var tillräckligt med skydd. I samma undersökning visade det sig att 82 % rapporterade att deras skrivbordsmiljö var för närvarande infekterade av spyware. Detta visar inte bara den stora spridningen på spyware utan också vilka brister företag har i kampen mot denna typ av hot (Baskin & Piltzecker, 2006).

2.3. Insider

En av de största källorna till problem inom informationssäkerhet är de egna anställda i företaget. De anställda som arbetar med programutveckling t.ex. har givetvis bra kunskap om programmen de varit med att utveckla och dess brister. Denna kunskap kan de sedan använda för att angripa systemet eller sprida informationen till en person utanför företaget som sedan angriper systemet. Dessa anställda har benämningen ”insiders”. (InfoSäkerhetsutredningen, 2004)

Det finns flera olika typer av insiders, det kan vara allt från anställda som anses vara väl betrodda i företaget till inhyrda konsulter. Oberoende vem det är har de en sak gemensamt, att de har tillgång till information som inte en vanlig utomstående person har. De kan enligt designen på systemet ha fått tillgång till informationen eller att de fått det genom ett misstag. (Contos, 2006)

Hur anställda blir insiders kan vara lite olika. Somliga har som avsikt att direkt skada företaget när de börjar. Deras avsikt att börja på företaget kan vara att föra ut information till en utomstående eller rent generellt sabotera. Personen kan både vara där en kort tid för att få tag i specifik information eller en längre tid för att ta sig upp i företagets hierarki. Denna form av attack associeras oftast med statliga organisationer eller stora betydande företag. De som går med i en organisation med avsikt att bli en insider utgör naturligtvis en väldigt betydande risk. (Contos, 2006)

Enligt undersökningar av vem som blir insiders är det oftast före detta anställda eller anställda som enbart är missnöjda med företaget och vill skada det på något sätt (Lundblad, 2005). Det är väldigt vanligt att en före detta anställd omedvetet har kvar sina fysiska kortnycklar, konton och lösenord. De flesta före detta anställda som blivit insiders blev antingen sparkade eller fick sluta. De som slutade fick troligtvis också sparken men det ser och låter bättre att säga att någon bara slutat. En annan sak som är väldigt intressant är att alla insiders nästan uteslutande är män (Contos, 2006).

De allra flesta människor har en gräns för när de kan mutas, vissa har en hög tröskel medan andra en låg. Av alla människor i världen har cirka tio procent en så hög moral att de brukar anses som omutbara. Det är inte bara pengar som kan spela roll utan även tillfället och situationen. (Syrén, 2005)

Insiders kan orsaka flera olika typer av skador mot ett företag som gör att de förlorar sekretessbelagda uppgifter, personuppgifter läcker ut, minskad dataintegritet, förlust av kunder, ekonomiska skador och naturligtvis att företagets rykte samt varumärke kan skadas (Contos, 2006). Det kan även leda till mänskligt lidande hos de andra anställda (Syrén, 2005). Trots att allt detta kan hända måste ett företag medvetet ta risken att någon av dessa saker kan inträffa. Det går inte att bara låsa in all information i ett kassaskåp för då skulle det vara helt omöjligt att utföra något arbete överhuvudtaget. Utan det de måste göra är att utvärdera riskerna för dessa händelser. För det finns inget företag som har de pengar och resurser det krävs för att säkerhetsställa alla servrar, nätverk, mobila enheter osv. utan de måste helt enkelt inrikta sig på att säkra de viktigaste systemen och den känsligaste datan. Det är alltså nödvändigt att förstå sig på riskerna som finns först för att sedan kunna hantera insiderhoten (Contos, 2006).

Den som utför ett insider hot behöver inte alltid göra det avsiktligt utan det kan även ske oavsiktligt. Det en insider gör är att bryta mot företagets säkerhetspolicy antingen avsiktligt eller oavsiktligt. Olämpliga insiderbeteenden är inte något som är nytt. Utan ungefär en tredjedel till tre fjärdedelar av alla anställda har någon gång deltagit i någon form av bedrägeri, skadegörelse, sabotage på arbetsplatsen. (Pfleeger et al., 2010)

Ett exempel på en oavsiktlig insider händelse var när Alex Greene år 2007 ville uppdatera sin prenumeration på Department of Homeland Security (DHS) intelligence bulletin med sin nya e-mail adress. När han skulle göra detta tryckte han på ”reply all” av misstag, vilket ledde till att mer än 2.2 miljoner e-mail skickades ut till ungefär 7500 statliga myndigheter och privata säkerhetsspecialister innan e-mailservern gick ner. Informationen i bulletinen är oklassificerad och prenumerationslistan är öppen men detta gjorde även att klassificerad kontakt- och departement information äventyrades. Individuella prenumeranter med säkerhetsklassificering hölls anonyma tills de också klickade ”reply” och därmed svarade från sina arbetskonton som automatiskt genererade signaturer som ofta innehöll telefonnummer och track-back data. Alla mottagare av Greenes mail fick en lista på försvarsministrets och Homeland securitys kontaktuppgifter. De läckta uppgifterna hade lätt kunnat missbrukas. (Pfleeger et al., 2010)

Det som gör insiderhot till ett stort problem är att vem som helst kan vara en insider. Detta beror på att det inte kräver några speciella kunskaper för att genomföra en informationsstöld. Det kan räcka med kunskap om hur in loggning går till på ett system och hur data kopieras. Med dagens teknologi är det även väldigt enkelt att genomföra detta, det är bara att koppla in sin mobiltelefon, mp3-spelare, USB-sticka i datorn och föra över stora mängder data och detta på mycket kort tid. För att sedan med enkelhet promenera ut obemärkt (Contos, 2006). Den här sortens hot är svåra att få bukt med då det egentligen rör sig om en personalfråga, hur rekryteringen går till och hur personen lämnar organisationen. De anställda som får för sig att begå ett insider brott är oftast de som känner sig illa behandlade av organisationen (InfoSäkerhetsutredningen, 2004).

2.4. Social engineering

Social engineering – konsten att luras, är något som företag ofta förbiser när de gör säkerhetsplaner även om det är ett av det farligaste och lättaste sättet att infiltrera ett nätverk (Dubrawsky, 2007). Social engineering används ofta eftersom det är mycket enklare att fråga någon efter information än att förbereda och genomföra en avancerad mjukvaru- eller hårdvaruattack för att komma åt information. Själva poängen med social engineering är att få offret att vara till hjälp. Attackerare utger sig ofta för att vara någon som arbetar inom organisationen (Pfleeger & Pfleeger, 2003).

De fysiska attackerna sker främst i den verkliga världen med syftet att samla in information som inte går att få tag i via andra källor. Denna typ av attack görs ofta för att underlätta en senare och mer avancerad attack. Några av de vanligaste fysiska attackerna är enligt Nohlberg (2008):

Dumpster Diving är när någon fysiskt går igenom någon annans papperskorg eller soptunna i hopp om att få tag i värdefull information. Det brukar ofta vara lätt att hitta kundinformation eller produktinformation, interna meddelanden och lösenordsinformation som slängts i papperskorgen. Anställda kan till och med slänga dokument som det tydligt står att de är för

”internal use only”, vilket innebär att bara anställda ska få ha tillgång till det. (Mitnich & Long, 2008)

Stöld av fysisk information, det kan vara att någon tar sig in i någons kontor och kopplar loss datorn för att sedan föra ut den från byggnaden. Datorn i sig innehåller ju information som kan vara av värde. (Nohlberg, 2008)

Tailgating är när en person följer en behörig person in i en byggnad och tar sig in tack vare det. För att ta ett exempel, det finns alltid någon som röker på ett företag och för att passa in kan en obehörig person klä sig likt de anställda samt ställa sig där de brukar röka. De kan stå utanför en bakdörr som de anställda måste ha nyckel för att ta sig in genom eller vad det nu kan vara. Ifall anställda står där och röker när de kommer ut och sen pratar lite med dem för att ge intryck att hör hemma där kan den obehöriga slinka in genom dörren när de andra går in. (Mitnich & Long, 2008)

Utpressning kan användas för att komma åt information. Det är möjligt att tvinga en person som har tillgång till information att ge ut den, detta kan ske genom våld eller hot. (Nohlberg, 2008)

Desktop Hacking innebär att någon letar upp nerskrivna lösenord som människor ibland lägger under tangentbord och liknande för att komma ihåg sitt lösenord (Nohlberg, 2008). De kan även använda sig av ”shoulder surfing” som är en klassisk icke teknisk attack som har funnits sedan urminnes tider. Denna typ av attack är väldigt enkel, det en attackerare gör är att ställa sig bakom ett offer och kika över axeln på denne för att se vad han eller hon gör. På detta viset kan en attackerare snappa upp en användares lösenord när det skrivs in på tangentbordet till datorn (Mitnich & Long, 2008).

De sociala attackerna använder i huvudsak sociala tekniker, men kan också använda tekniska hjälpmedel. Men det som kännetecknar en social attack är att den använder sig av någon form av bedrägeri för att lyckas. Ett klassiskt exempel på en social attack är att ringa den som skall attackeras och förklarar att det är något problem med nätverket samt ber om hjälp för att lösa det. Den som blivit uppringd kommer att tycka det är alldeles för komplicerat och attackeraren erbjuder då snällt att hjälpa till om de ger ut login informationen till systemet (Nohlberg, 2008). Det attackeraren gör är att helt enkelt lura åt sig informationen och just detta angreppssätt är en favorit hos attackerare när det gäller social engineering (Gollmann, 2006).

Sociala attacker kan också utföras med hjälp av tekniska hjälpmedel som e-mail eller snabbmeddelande som t.ex. Windows Live Messenger[2]. I en sådan attack skulle attackeraren försöka få en person till att klicka på en viss länk eller installera ett malware program. Den största delen är alltså att lura någon och inte den tekniska biten. (Nohlberg, 2008)

Det finns även en kombination av tekniska och sociala attackmetoder som t.ex. ”Road Apple”. Ett road apple kan vara att en person preparerar ett USB-minne och lägger in någon skadlig kod på det för att sedan lägga det på något ställe som någon kan ”hitta” det på. Det attackeraren sedan hoppas på är att den personen som hittat det ska plugga in det i sin dator och där med infekteras av den skadliga koden. (Nohlberg, 2008)

[2] Windows Live Messenger är Microsofts klientprogram för direktmeddelanden som ingår i deras användarplattform Windows Live.

2.4.1. Spoofing

Spoofing innebär att ge ut falsk information om sin identitet för att kommer åt ett system som personen inte är behörig till. Personen utger sig för att vara någon annan än vem han/hon är helt enkelt. (Dubrawsky, 2007)

För att identifiera och autentisera sig i ett system används ofta användarnamn och lösenord. Men det finns ett problem med detta och det är att användaren inte kan veta helt säkert vem som tar emot lösenordet. Det är just detta som attackerare utnyttjar genom att använda sig av spoofing. För att ta ett exempel, när en användare ska logga in på sin dator möts han av en inloggningsskärm där han får mata in lösenord. Men det han inte vet är att en person varit där och lagt in ett spoofing program som visar exakt samma inloggningsskärm som operativsystemet visar. Detta program startas automatiskt i samband med att datorn startas och när användaren då matar in sitt lösenord kommer ett felmeddelande visas att något gått fel med inloggningen. Spoofing programmet stängs nu ner och den riktiga inloggningsbilden visas. Användaren matar då in sitt lösenord igen i tron att han bara slagit fel lösenord första gången och tänker inte mer på det. Det som nu har hänt är att användarens uppgifter har lagrats åt attackeraren utan användarens vetskap. Skadan som blivit i och med detta kan vara enormt stor beroende på vems konto attackeraren kommit åt. Han får som sagt tillgång till att logga in och kan då nå viktig information tack vare detta. (Gollmann, 2006)

Det går att skydda sig mot denna typ av spoofing attack genom att på något sätt visa för användaren antalet misslyckade inloggningar som har gjorts. För om inloggningen nu misslyckas och det fortfarande står att inga login försök har misslyckats bör användaren definitivt bli misstänksam. Det går även att använda sig av en trusted path som är en säker väg för inloggning. I Windows kan du få upp denna genom att trycka ctrl+alt+del och detta ska göras även om inloggningsskärmen är synlig. På detta viset undviks risken att bli utsätt för en spoofing attack. (Gollmann, 2006)

Något som är ett väldigt stort problem idag på Internet är all spam. Det många attackerare ofta använder sig av är en metod som kallas för e-mail spoofing. Vilket innebär att de ändrar själva ”from” fältet i e-mailet för att få det att se ut som mailet kommer från en säker domän. Detta görs för att få e-mailet att verka trovärdigt och upplevas säkert av mottagen att öppna. Det som sker är att någon försöker lura mottagaren att öppna e-mailet och sedan klicka på en länk i meddelandet eller öppna en bifogad fil som de även där döpt till ett lämpligt namn. Det användarna inte vet är att om det trycker på länken eller öppnar den bifogade filen är att de utsätter sig för någon form av attack som ett virus. (Dubrawsky, 2007)

Det finns även e-mail spoofs som kallas för sociala virus. Ett exempel på ett sådant mail är t.ex. varningsmeddelande om att det finns något virus ute som de skall akta sig för och där mottagaren då rekommenderas att skicka vidare detta till sina adresskontakter för att informera dem. Den här typen av mail brukar inte i sig vara farliga utan de brukar oftast leda till att nätet blir överbelastat av alla mail som skickas. Det finns inget virus utan det är själva spam mailet som är viruset. Detta kan då hindra annan viktig information att nå fram eller sega ner hela nätet vilket stör systemet. (Lundblad, 2005)

Att utföra en e-mail spoof är väldigt enkelt, men kan vara svår att hindra. Det bästa företag och andra kan göra för att hindra sådana här hot är att utbilda användarna angående de här hoten samt att ha en bra konfiguration i mail programmen för att sortera bort de värsta spamen (Dubrawsky, 2007). Det är viktigt att inse att bara för att det står att mailet kommer ifrån en

känd person behöver det inte betyda att det är från honom. Det räcker att den som blivit utsatt för ett virus har en person i sin adressbok så kan ett virus mail skickas ut i dennes namn (Lundblad, 2005).

En annan typ av spoofing attack är website spoofing. Den här typen av spoofing innebär att en attackerare skapar en webbsida som är väldigt lik, ibland nästan helt identisk en annan sida. När de skapar sådana här spoof sidor återskapar de endast det som är nödvändigt för att skapa illusionen att det är den äkta sidan. Då det oftast finns avancerade system bakom själva sidan som hade tagit för lång tid att återskapa och användarna ser ändå inte detta. De webbsidor som oftast utsätts för detta är av typen e-handel, bank eller gambling. (Dubrawsky, 2007)

Något som attackerare ofta utnyttjar är URL förvirring dvs. att utnyttja förvirringen hos användare angående domännamnet till en webbsida. Om det finns ett företag som har domännamnet citibank.com t.ex. så kan en identisk sida med adressen citybank.com sättas upp. Det är nämligen ganska vanligt att användare skriver in fel i adressfältet på webbläsaren eller rent av tror att det är den adressen då de är väldigt nära varandra. Det de kan göra för att locka användare till sin sida är att köpa annonser som länkar till sidan, reklam på andra sidor med länk, skicka ut e-mail med information om sidan. (Pfleeger & Pfleeger, 2003)

Själva huvudsyftet med denna sortens attack är att komma åt en användares uppgifter. Det kan vara användarnamn och lösenord men även saker som PIN-kod och kreditkortsnummer. Om en sida utsatts för en spoofing attack kommer användaren som försöker logga in på sitt konto att lämna ut sina uppgifter till attackeraren (Dubrawsky, 2007). När insamlingen av informationen är tillräcklig kan antingen sidan stänga ner, fortsätta samla in information eller skicka vidare användaren till den riktiga sidan. Det finns även möjlighet till att skicka vidare användaren till den riktiga sidan och logga in användaren där utan att denne märker att den blivit lurad (Pfleeger & Pfleeger, 2003). När attackerarna väl fått tag i uppgifterna för en giltig användare kan de utföra alla typer av förstörelse på deras konto (Dubrawsky, 2007).

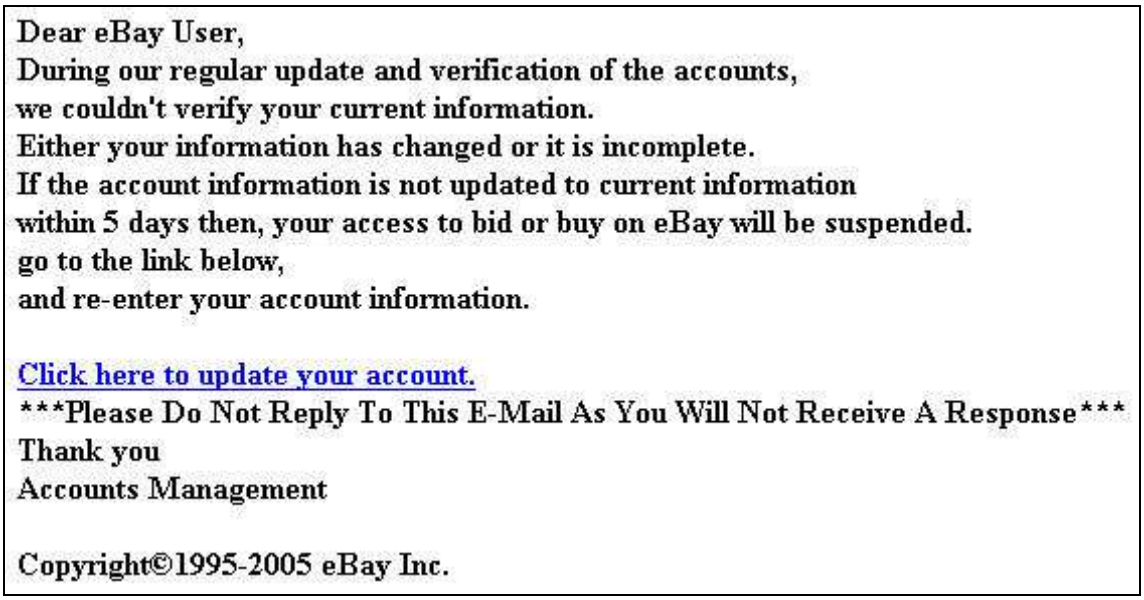
För att göra en sådan här attack behöver de inte göra en kopia på en annan befintlig sida för att genomföra detta. Utan de kan även välja att göra en sida som är väldigt trovärdig och ser legitim ut. För att sedan lura användaren att ge ut sitt kreditnummer eller bara få tag i användarinformation för de som registrerar sig. (Pfleeger & Pfleeger, 2003)

2.4.2. Phishing

Phishing är en kriminell mekanism som använder sig både av social engineering och tekniska undanflykter för att stjäla konsumenters personliga identitetsdata och finansiella kontouppgifter. (APWG, 2009)

Ordet phishing kommer från ordet fishing (fiske) och syftar på att attackeraren kastar ut ”krokar” som han sedan hoppas att några ”biter” tag i. Det är precis så den vanligaste formen av phishing fungerar men det är mail som ”kastas” ut. Förfalskade e-mail skickas till mottagare i mängder och felaktigt utge sig för att vara ett berättigat driftställe, för att försöka lura åt sig personlig information som kreditkortnummer eller lösenord till bankkonton. I de flesta fallen står det i e-mailen att mottagaren ska besöka en hemsida för att fylla i personlig information. Men för att lyckas med detta måste de få mottagarens förtroende att de är det berättigade företaget. Det får de genom att skapa en hemsida som är designad för att se ut som det riktiga företagets sida, men vilket det i själva verket inte är. De kommer att ta den personliga informationen för egen vinning. (Stewart & James, 2005)

En phishing attack kan gå till på följande sätt. Attackeraren börjar med att skicka ut spam-mail (se figur 2:1 för exempel) till massvis med konton som tillhör en sida, där de utger sig för att vara de som administrerar användarkontona på sidan. I meddelandet uppmanar de användaren att klicka på en länk för att komma till sidan där de kan logga in och ändra sina användaruppgifter eller liknande. När de sedan matar in sina uppgifter på sidan kommer attackeraren få dess inloggningsuppgifter och oftast skickas även användaren vidare till den riktiga sidan utan att ha förstått att den blivit utsatt för en attack. Bästa sättet att skydda sig mot sådana här hot är att kontrollera URL adressen osv. för att då kunna se att den verkligen går till rätt sida. (Dubrawsky, 2007)


Dear eBay User,
During our regular update and verification of the accounts,
we couldn't verify your current information.
Either your information has changed or it is incomplete.
If the account information is not updated to current information
within 5 days then, your access to bid or buy on eBay will be suspended.
go to the link below,
and re-enter your account information.

Click here to update your account.
Please Do Not Reply To This E-Mail As You Will Not Receive A Response
Thank you
Accounts Management

Copyright©1995-2005 eBay Inc.

Figur 2:1. Ett exempel på hur ett phishing mail kan se ut (Nohlberg, 2008 s.61).

Spear phishing är en relativt ny teknik som skiljer sig en del från vanlig phishing. I spear phishing använder attackeraren sig av väldigt riktade e-mail istället för att skicka ut till den breda massan. Det huvudsakliga målet är att lura mottagaren att tro att det är någon den verkligen känner. Målet med denna attack är givetvis precis som phishing att komma åt information från en person, men även att komma in i en organisations datorsystem. Det är just detta som gör denna typ av phishing extra farlig samt att det är förmodligen denna variant professionella attackerare föredrar. Något som gör en sådan här attack ännu farligare är om mottagaren väntar svar från den personen attackeraren utger sig att vara. Sådan här information kan t.ex. letas fram via sociala nätverk, vilket ibland kallas för social phishing. (Nohlberg, 2008)

APWG Chairman Dave Jecans sa,”Spear-phising and whale-phishing, where targeted individuals inside of corporations, or of his net worth, appears to be increasing. Phishers and malware attackers are sending emails to individuals in a highly targeted fashion, attempting to gain access to corporate online banking systems, corporate VPN networks, and other online resources”. (APWG, 2009)

2.5. Olyckor och misstag

Arbete med informationssäkerhet handlar mycket om att hindra hot. Det är dock viktigt att komma ihåg att säkerhetsarbetet även innehåller förberedelser för att förhindra olyckor, men

det som är svårt angående olyckor är att förutse dem. Det företag kan göra för att förebygga dem är att ha allmänna regler som minskar den skada som olyckor kan ställa till med. Det kan vara regler som att personer inte får dricka någon vätska i serverrummet och all information ska det köras backup på. Men det går absolut inte att förebygga alla sorters olyckor utan det gäller att istället sätta upp hur de ska agera när olyckan har inträffat. (Lundblad, 2005)

Vid utvecklingen av ett system kan ett fel uppstå i själva programutvecklingen vilket kan leda till att information försvinner eller att systemet rent generellt utsätts för störningar och därmed störa verksamheten (InfoSäkerhetsutredningen, 2004).

Något som kan vara komplicerat är när datorutrustning och program ska installeras eller uppgraderas. Det är viktigt att göra detta korrekt annars kan detta leda till störningar dvs. systemet kan vara nere under en viss tid vilket gör att användare inte kan få tillgång till den information de behöver för att utföra sitt arbete. Att en sådan här incident inträffar kan bero på dålig kompetens eller utbildning hos dem som utför arbetet. (InfoSäkerhetsutredningen, 2004)

Det kan vara enkla saker som att en anställd gör ett administrativt misstag. Ett exempel kan vara att de glömmer att ta bort en före detta anställds konto och rättigheter när denna person slutar på företaget. Den före detta anställde kan då anses som en risk och ett hot då han kan ta sig in i systemet och komma åt information, vilket kan leda till att denne sprider ut viktig information till andra obehöriga. (InfoSäkerhetsutredningen, 2004)

Något som det alltid finns risk för är brand och översvämningar på en arbetsplats. Vid översvämning finns det ofta bra med tid att reagera dvs. stänga ner alla datorsystem och säkra dem. Men om ett vattenrör brister på fel ställe kan det gå väldigt snabbt och orsaka stora skador. I förebyggande syfte kan det finnas plastpåsar och vattentålig tejp nära till hands om ett vattenrör skulle brista så att det går temporärt täcka över. Det är viktigt att ha kontroll och veta vad olika personer skall göra så att den viktigaste datan inte försvinner. Ett sätt är att märka hårddiskar med etiketter som grön, gul, röd för att visa vilka som innehåller viktigast information och om det sedan är storm eller liknande så skall de röda som står för den viktigaste föras till en säker plats. (Pfleeger & Pfleeger, 2003)

Som tidigare nämnt finns det alltid risk för naturkatastrofer som t.ex. stormar som kan skada företagets byggnader. Det finns risk att denna typ av incidenter kommer att öka i framtiden pga. den globala uppvärmningen som bidrar till klimatändringar. Detta kan spela en stor betydelse för många företag. Skador kan innebära att företaget tappar kunder och marknadsandelar. Stormen Gudrun som inträffade i december 2004 resulterade i att många i södra Sverige blev utan ström och telefon. Natten efter var 258 000 kunder utan ström och det tog lång tid innan alla hade det igen. Detta kostade pengar för alla som drabbades och elbolagen fick skadeståndskostnader på flera hundra miljoner. (Syrén, 2005)

Brand är mer allvarligt än vad översvämningar är då de ofta ger en mindre tid till att reagera och att någon människa kan skadas ökar. Det är viktigt att skapa rutiner för hur anställda ska reagera, att vissa stänger av system och andra stänger dörrar, kabinetter med mera. Ett problem med eld är hur släckningen ska gå till då vatten som vanligtvis används inte är en så bra idé då det kan göra ytterligare mer skada på datorkomponenterna. Därför är det vanligt förekommande med koldioxidbrandsläckare och system som sprutar ut gas i byggnaden. Problemet med dessa system är att de går ut på att ta bort syret i luften vilket då innebär att det kväver eventuella människor som inte hinner ta sig ut. Därför är det viktigt att alla tar sig

ut innan dessa används. Det ska även finnas få fönster till serverum och branddörrar som hindrar elden för att spridas. (Pfleeger & Pfleeger, 2003)

Något som all elektronik behöver är elektricitet och det är konstant. När det blir strömavbrott innebär det att allt går ner och det direkt. Det innebär att allt som alla arbetar med just då eller inte har sparat kan försvinna. En del komponenter kan även ta skada av att strömmen försvinner hastigt, därför drar t.ex. hårddiskars läsnål bort sig vid hastiga strömavbrott (Pfleeger & Pfleeger, 2003). De flesta företagen idag är väldigt beroende av fungerande elkraft, telefoni och Internet för att kunna vara verksamma. Men ändå är det relativt få företag som har någon slags UPS[3] som går igång vid strömavbrott och ger elkraft (Syrén, 2005).

Ström är mycket viktigt för ett företag för att fungera och för att belysa detta kan man bara se på hur SSAB Tunnplåt i Borlänge drabbades 2005 när strömmen gick ner 1 timme och 20 minuter. Detta relativt korta avbrott kostade företaget cirka 20 miljoner kronor, dels för att de förlorade produktion men även för att maskiner gick sönder. (Syrén, 2005)

En vanlig olycka på ett företag kan vara att en anställd har en kaffekopp med sig till sin arbetsplats men råkar välta koppen rakt över datorn som kortsluts och stängs av. Risken finns att informationen på hårddisken kan vara förstörd. (InfoSäkerhetsutredningen, 2004)

Antivirusföretaget McAfee gjorde nyligen ett misstag som drabbade flera företag och användare. Det som hände var att de klassificerade en Windows systemfil som virus vilket ledde till att när uppdateringen installerades stängdes datorn av och starta bara om sig hela tiden. Att antivirusföretag av misstag klassificera filer som virus som inte är det händer ofta men nu var det en Windowsfil vilket innebar att alla datorer som kört uppdateringen behövde åtgärdas var för sig för att få igång dem igen. Detta ledde ju till att de företagen som drabbades stod still. (Brandell, 2010)

2.6. Risker och hot med mobila enheter

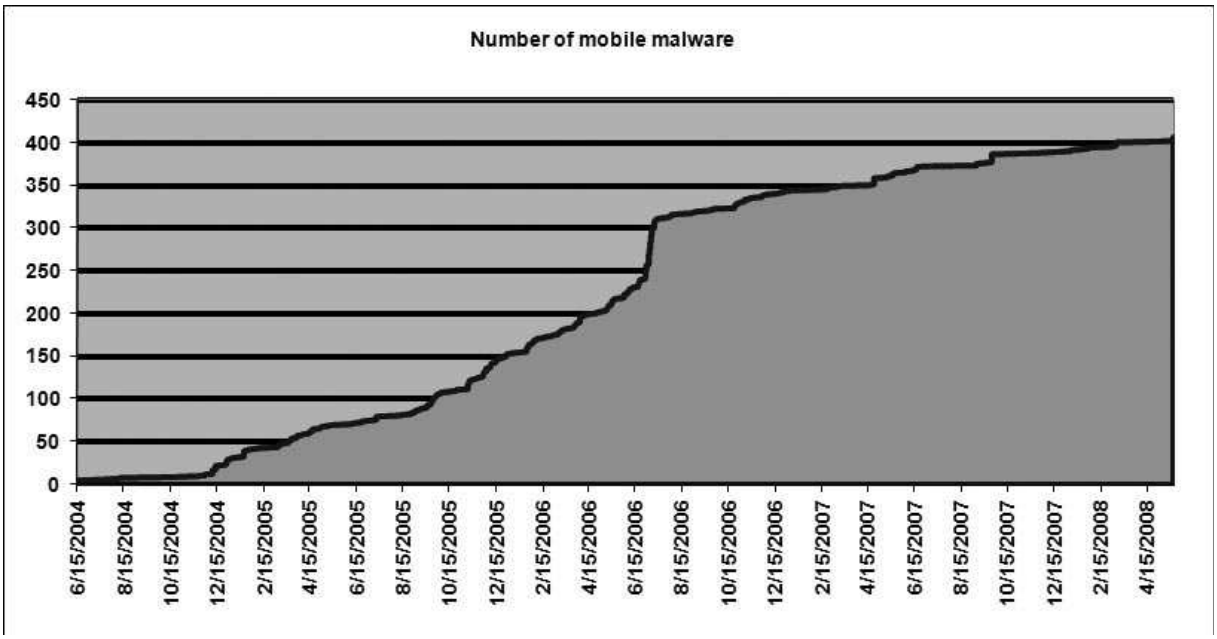
Företagen idag blir allt mer mobila när det gäller var de anställda arbetar ifrån. Det innebär att det är väldigt viktigt för företag att ta med mångfalden av teknik i sin informationssäkerhets-planering. Idag kan anställda använda handdatorer, bärbara datorer, mobiltelefoner i sitt arbete och detta är bara några av de många tekniska hjälpmedel som finns att tillgå som kan innehålla information från företaget. Därför är det viktigt att ha specifika åtgärder även för dessa. Det kan vara guld värt för en konkurrent att få tag i en bärbar dator då den kan innehålla interna hemligheter om företaget. Trots att denna risk finns är det många företag som inte har några speciella regler för vad som får finnas på mobila enheter och hur den ska skyddas samt hanteras vid resor. (Lundblad, 2005)

Nu för tiden är mobiltelefoner, handdatorer och bärbara datorer en stor del av företagens verksamhet. De behövs också för att företagen ska kunna bedriva sin verksamhet på ett effektivt sätt. Men trots detta görs det väldigt få analyser av hur sårbara mobiltelefoner och handdatorer är. Finns det t.ex. bluetooth igång på mobiltelefonen finns det risk att bli attackerad av någon som står nära. En attackerare kan genom bluetooth komma åt hela en persons kontaktlista. Allt eftersom nya funktioner tillkommer i mobiltelefoner och bärbara

[3] Uninterruptible power supply är en elektrisk apparat som ger reservkraft när det vanliga elnätet går ner. De skyddar normalt även mot spänningsspikar i elnätet som det kan bli vid åskväder.

datorer ju mer sårbara blir de. Det är säkerheten som blir lidande för alla nya funktioner, men ibland kan det vara värt det också då det gör att de tjänar mer på det än vad risken är. Många mobiltillverkare uppmanar användare att använda funktioner som kodminne som ger användare möjlighet till att lagra koder och lösenord. Detta är inte så bra om de mot förmodan skulle tappa den och den hamnar i fel händer. (Lundblad, 2005)

Den mobila marknaden av smartphones har växt explosionsartat de senaste åren. I takt med den växande mobila marknaden har även cyber-kriminella bedrägerier och spridningen av mobila malware ökat. Mobila malware har ökat stadigt sen år 2000, men enligt F-Secure Corp. har de ökat markant från 2004 och framåt som kan ses i figur 2:2. Med en global explosion av mobila lösningar och tjänster är tillgångar allt mer integrerade i detta framväxande medium. De kriminella utnyttjar redan detta för finansiell vinst. Detta problem kommer säkerligen att bli värre innan det blir bättre då denna nya marknad mognar för ett allt mer rörligt globalt samhälle. (Dunham, 2009)



Figur 2:2. F-Secure Corp. Undersökning visar en betydande ökning i mobila malware (Dunham, 2009 s.6).

En vd på ett företag behöver kanske ha en BlackBerry för att ringa samtal i arbetet, surfa på webben, ta emot och skicka e-mail samt se på bifogade filer i mailen. Om hans enhet skulle attackeras kan de få tag i hans kontakter för att sedan attackera dem eller de kan få tag i viktiga företagsmail som attackerare kan använda eller sälja till konkurrenter. (Dunham, 2009)

Något som många nu har är portabla mp3-spelare som iPod, Philips och Creative. De moderna spelarna har en väldigt stor lagringskapacitet och används ofta också som portabla lagringsenheter. Då fler och fler tar med dessa till jobbet och pluggar in dem i datorerna ökar risken för spridning av virus och industrispionage. (Lundblad, 2005)

Säkerhetsföretaget Thales gjorde en undersökning om den brittiska regeringens datoranvändning och säkerhet. Det visade sig att Försvarsdepartementet i Storbritannien förlorade 594st bärbara datorer mellan 1996 och 2002. Enligt företaget innehöll så många som 60st känslig information. Men de började inte göra säkerhetsåtgärder förrän 2003 och pga.

undersökningen. Det finns skrämmande exempel på där bärbara datorer försvunnit som innehöll känslig information som t.ex. när en MI6-agent glömde sin bärbara dator i en taxi. Som tur är går det att skydda informationen med hjälp av diverse produkter, som att kryptera hårddisken. Kryptering gör det betydligt svårare för någon att få tillgång till att läsa informationen. (Lundblad, 2005)

3. Metod

3.1. Tillvägagångssätt

Arbetet började med att studera litteratur och teorier om hot mot informationssystem. Dessutom studerades vilka åtgärder som görs för att förhindra dessa hot samt vilka konsekvenser de skulle kunna få för företagen om de utlöstes. Detta gjordes för att samla fakta och få ett underlag till den empiriska studien. Studien av litteratur visade att det fanns ett ökat antal och en större mångfald av hot mot informationssystem. Det medför nya säkerhetsproblem för företag som behöver veta vad som är orsak till hoten och hur det går att skydda sig emot dem. Det var några hot som var mera frekvent förekommande i litteraturen. De fanns också med på olika listor över hot mot företag/organisationer. För att den redovisade litteraturgenomgången inte skulle bli för omfattande begränsades denna till de mest förekommande hoten.

3.1.1. Litteraturgenomgång

Litteraturfördjupning är ett sätt att se vad som det har forskats om och publicerats inom området tidigare. Därför gjordes det en systematisk litteratursökning vilket är mest lämpligt då det söks litteratur om ett specifikt område (Rienecker och Jorgensen, 2008). Syftet med litteraturinsamlingen var att få fram fakta för att kunna besvara frågeställningarna och utveckla ett underlag till frågeformuläret. För litteratursökningen användes Lunds universitetsbiblioteks elektroniska resurser, katalogen Lovisa och Elin@lund. Sökningen gjordes för att finna böcker, e-böcker, vetenskapliga artiklar, avhandlingar och tidskrifter som uppfyller kraven på akademisk validitet samt reliabilitet. Det gjordes även sökning i google och google scholar som komplement. Information från Internetsidor kan ha olika tillförlitlighet. Det har använts källor med bättre tillförlitlighet som myndigheters hemsidor och facktidskrifter.

Källorna måste bedömas för att se om de är giltiga och relevanta för det som undersöks. Dessutom måste källorna vara tillförlitliga och trovärdiga enligt Jacobsen (2002). Det har därför i litteraturgenomgången i första hand använts litteratur som bygger på forskning och från myndigheter.

3.1.2. Empiriska studier

För att få ytterligare information som syftar till att besvara min forskningsfråga har det genomförts en undersökning där det använts ett frågeformulär. Tretton företag tillfrågades om de kunde svara på frågor angående hot mot deras informationssystem. Av dessa tretton företag som kontaktades svarade tio på min förfrågan. Två svarade tydligt att de ej ville delta, en svarade att de inte ville vara med då de såg risker med att lämna ut informationen, en ville inte besvara frågorna utan ville hellre föra en diskussion över telefon. Därefter skickades intervjufrågeformuläret via e-mail till de kvarvarande sex företagen. Det ena företaget kunde

inte svara så utförligt då de hade en hel del sekretess regler angående dessa frågor. De andra kunde svara men ville vara anonyma för att inte kunna kopplas till denna uppsats. Därför har det inte gjorts någon redovisning och beskrivning av företagen eller av de personer som svarat på intervjufrågeformuläret.

Efter det att företagen besvarat frågeformuläret och återsänt dem via e-mail kontrollerades att de besvarat samtliga frågor. I två fall behövdes en komplettering till en av frågorna. Svaren avidentifierades så att de blev anonyma. Den data som framkom vid undersökningen har redovisats och sammanställts.

3.1.3. Analys och diskussion

När det insamlade materialet från frågeformuläret sammanställts behövdes ett angreppssätt för att analysera resultatet. Resultatet i Empirin har redovisats under olika teman med utgångspunkt från forskningsfrågan och det teoretiska underlaget. Rubrikerna har fungerat som ett verktyg där de olika temana kategoriserats. I analys och diskussion har använts samma teman och därmed samma rubriker. Jag har kunnat undersöka resultatet av det insamlade materialet och placera svar samt resonemang under rätt rubrik. Det har därmed gått att urskilja det som ansetts extra intressant.

3.1.4. Slutsats

I slutsatsen redovisas svaren som arbetet kommit fram till på forskningsfrågan. Vidare utvärderas det om syftet med studien och koppling till forskningsfrågan. När en problemställning undersöks kan det ge upphov till nya frågeställningar. De frågeställningarna redovisas under rubriken fortsatt forskning.

3.2. Metodval

I denna uppsats har det valts att samla in empirisk data genom en kvalitativ undersökning. Undersökningen har utformats som en form av små-N-studier. Enligt metodlitteraturen ges enheter ofta beteckningen N (Jacobsen, 2002). Studien innebär att endast några få enheter undersöks där fokus finns på ett specifikt fenomen eller område. Några få företag kan då undersökas mer, för att få en insikt i vilka hot som företagen ser mot sitt informationssystem. I undersökningen har det används ett frågeformulär med frågor i fast ordningsföljd med möjlighet till öppna svar.

För att få reda på vilka de största hoten mot ett företags informationssystem är ställdes det frågor till personer som arbetar med informationssäkerhet på olika företag/organisationer. Då de har kunskap om vilka hot som kan förekomma mot just deras företag. De har även information om hur de ska agera mot dessa hot samt vilka konsekvenser de kan komma att ha för företaget.

Frågeformuläret sändes ut till sex olika företag. Syftet med detta var att få en bild över vilka de största hoten mot företag är, hur personer kan vara säkerhetsrisker, vilken utbildning och information anställda får samt vilka regler och restriktioner som finns för anställda.

3.3. Urval

För att göra ett urval gjordes en lista över företag/organisationer som var lämpliga att ingå i undersökningen. Det huvudsakliga kriteriet var att företaget skulle ha en person som arbetade med IT och var insatt i företagets informationssäkerhet. Detta ger en förutsättning för att få lämpliga företag till undersökningen. Valet av företag gjordes genom att fråga företag som låg geografiskt nära samt där jag hade en kontakt med insyn i företaget. Detta för att lättare komma i kontakt med en person som kunde besvara frågorna. För att arbetet med uppsatsen inte skulle bli allt för omfattande och då undersökningstiden är begränsad valdes tretton företag ut. De deltagande företagen har fått full anonymitet (se kap 3.6) och därför görs ingen presentation av dem.

3.4. Frågeformulär

Frågorna har successivt arbetats fram allt eftersom litteraturgenomgången fortgått. Samtliga frågor har utarbetats med utgångspunkt från litteraturgenomgången. Presentation av frågorna finns i Bilaga B1. Ett syfte med frågeformuläret var att utforska hur företag ser på hot mot deras informationssystem och identifiera vilka hot som de ser som de största samt vad gör för att hantera dessa hot och vilka konsekvenserna blir om de genomförs. Ett viktigt led vid utformningen av frågorna var att ställa öppna frågor. Öppna frågor ger uppgiftslämnarna en möjlighet att utveckla sina svar och även en möjlighet att fånga upp oväntade synpunkter. Frågor som kan besvaras med ja eller nej får alltid en följdfråga som skall ge svar på varför det är så. Det har också varit av intresse av att ta reda på vilka regler som gäller för de anställda när de använder datorer och mobila enheter som kan påverka företagets informationssystems säkerhet.

3.5. Kritik av undersökningen

Den valda undersökningsmetoden skall samla in empiri som är giltig och relevant (valid) samt tillförlitlig och trovärdig (reliabel) enligt Jacobsen (2002).

Jacobsen (2002) anser att det finns ett grundproblem vid alla intervju- och frågeformulärsundersökningar eftersom personen som ingår i undersökningen inte direkt har någon skyldighet att svara. Det kan skilja mellan vad en person svarar och den faktiskt anser eller utfört. En fråga som Jacobsen (2002 s.447) anser att den som utformar ett frågeformulär alltid skall ställa är ”Har uppgiftslämnaren något att vinna på att ljuga?”. Uppgiftslämnarens kunskap om ämnet har stor betydelse för hur den svarar. Bra kunskap hos den som svarar ger mindre risk för att de svarar på måfå. Även hur frågorna ställs har betydelse. Mycket konkreta frågor ger bättre tillförlitlighet än frågor där personen som svarar skall tycka till och värdera. (Jacobsen, 2002)

Uppgiftslämnarna som ingick i undersökningen hade alla tjänster som kräver att de har kunskap inom området. Detta ger en möjlighet till att de svarar fullständigt och sanningsenligt. Frågorna i undersökningen är öppna och konkreta vilket också ökar möjligheten till att uppgiftslämnaren svarar fullständigt och sanningsenligt. Frågeställningarna kan dock vara känsliga och kännas besvärande för företaget/organisationen vilket kan

innebära en risk att uppgiftslämnaren medvetet utelämnat fakta vilket kan påverka resultatet. Företagen/organisationerna har dock svarat likartat på ett flertal frågor.

Det som är negativt med undersökningen är att det är så få företag som ingår i undersökningen. Det var dessutom några som inte gav några svar och detta beror då på att det är ett känsligt ämne inom vissa företag.

Det faktum att endast 46 % av företagen svarade utförligt på alla frågor och det från början var få företag kan utgöra en negativ påverkan på resultatets validitet.

Det hade varit bra att kunna intervjua fler företag och då fått fler svar på samma fråga. Det hade också varit bättre att göra intervjuerna på företagen vilket hade gjort det möjligt att ställa följdfrågor samt se hur personen reagerar på de olika frågorna.

För att pröva tillförlitligheten kan samma frågeformulär skickas ut en gång till några uppgiftslämnare för att se om det lämnas samma svar (Jacobsen, 2002). Detta har dock inte varit möjligt dels för att tiden varit för kort och dels för att de svarat på e-post och då kan ha svaren kvar.

3.6. Etiska aspekter

Jacobsen (2002) diskuterar de grundkrav som en undersökning skall uppfylla som informerat samtycke och krav på privatliv samt krav att bli korrekt återgiven. De utvalda företagen som ingår i undersökningen tillfrågades via e-mail om de ville vara med och svara på frågeformuläret om informationssäkerhet. I begreppet informerat samtycke ingår enligt Jacobsen (2002) att den som undersöks gör det frivilligt. De företagen som ingår i undersökningen svarade ja, ett företag svarade men ville inte vara med övriga svarade inte alls.

Rätt till det privata, i detta fall det enskilda företaget, är också något som det diskuteras kring när det gäller etiska dilemman (Jacobsen, 2002). När det gäller känslig information är det viktigt att ta hänsyn till att de deltagande företagen får full anonymitet vilket också var ett krav från företagen för att svara på mitt frågeformulär. Det innebär att svaren måste presenteras så att det för en utomstående inte är möjligt att identifiera företagen. För att det inte skall vara möjligt att identifiera företagen har viss data eliminerats. Därför benämns de företag A, företag B osv.

Det tredje kravet är att bli korrekt återgiven. Företagens svar på frågeformuläret återges och redovisas i bilagan. Data som kan bidra till identifikation kan ha tagits bort. Det som tagits bort har inte någon betydelse för de redovisade svaren.

4. Empiriska studier

I detta kapitel tas den data upp som är intressant för uppsatsen. För detaljerad empirisk data se bilagor B2-B7. Ett frågeformulär (se bilaga B1) skickades ut till sex företag och av dem som svarade var det fem som svarade på frågorna och den sjätte svarade att de flesta av frågorna som ställdes var sekretessbelagda och svarade därmed bara kort på några frågor.

4.1. Hot mot företagets informationssystem

Först bör nämnas att Företag A:s IS/IT-miljö sköts av ett externt företag, men att IS/IT-säkerheten styrs av företag A säkerhetsansvarige som i sin tur ger direktiv till det externa företaget.

Företag A rangordnade följande fem hot som de största mot sitt företag:

1. Virusangrepp
2. Intrång via nätet
3. Inbrott eller obehörig vistelse i lokalerna
4. Användarmisstag
5. Misstag från IS/IT-support

De åtgärder som företag A har gjort för att förhindra dessa hot är att utrusta alla datorer med antivirusprogram och brandväggar. Både antivirusprogrammet och brandväggen uppdateras dagligen för att det senaste skyddet alltid ska finnas på systemen. De gör även hela genomsökningar med antivirusprogrammen av systemen veckovis, för att säkra att där inte ligger något virus eller liknande på systemen. De använder precis som många andra företag sig av Microsofts produkter och programvara. Dessa måste alltid ha den senaste versionen för att stå emot hot som finns och därför har de automatisk uppdatering av deras programvara. Något som de även har valt att göra är att bemanna sin reception på företaget med ett externt säkerhetsföretag, detta för att stärka säkerheten ytterligare in till byggnaden. De har även valt att byta ut viss hårdvara som deras switchar och bytt dem till loop-säkra switchar för att undvika loopar för redundans i nätverket.

Angående vilka konsekvenser dessa hot hade fått om de genomförts mot företaget svarade de att attackerare skulle kunna få tillgång till företagshemligheter. Men även då vid sabotage kan det medföra att projekt som är pågående blir försenade tack vare detta och att det då leder till ekonomiska konsekvenser.

För att kunna försvara sig mot hot måste företaget veta vilka säkerhetsriskerna är och detta har företag A en separat avdelning som arbetar med just detta. Men de gör även lokalt på företaget en riskanalys av deras egen utrustning, den som inte sköts av det externa IS/IT-företaget.

Företag B rangordnade följande fem hot som de största mot sitt företag:

1. Trojaner
2. Lösenordsstöld
3. Virus
4. Diskkrascher och misstag
5. Systemstop och nätfel

Företag B har även de antivirusprogram och brandväggar på varje dator samt på alla deras servrar. Något som de också har valt att ha är olika nivåer på brandväggen i nätverket. De har även kontinuerlig övervakning över deras nätverk för att kunna analyserar och upptäcka ovanliga händelser i nätverket. All deras trafik i nätverket samt deras mailtrafik loggas för att upptäcka t.ex. phishing. De har även valt att reglera åtkomsten till deras filservrar hårt för att minska risken för obehöriga att ta sig in och för att minska antalet personer som rör sig omkring den. Företag B skickar även ut information angående hot som användarna på företaget ställs mot. Om det t.ex. sprids ett mail med virus på nätet meddelas användarna om detta och hur de ska agera.

Angående vilka konsekvenser hoten kan få för företag B är det samma som gällde för företag A dvs. att viktig information kan läcka ut och att sabotage kan leda till att projekt fördröjs samt att det kan ha ekonomiska konsekvenser.

Hur ofta företaget gjorde analyser av säkerhetsrisker kunde han tyvärr inte svara på då det låg helt hos säkerhetschefen.

Företag C hade som sagt sekretess på det mesta vilket innebar att det inte blev många ingående svar på frågorna. Men de svarade att de hade de vanligaste hoten och integritetshot samt avlyssning. Angående hur de åtgärdade dessa hot kunde de endast svara utbildning medan de resterande lösningarna låg under sekretess.

Företag D rangordnade följande fem hot som de största mot sitt företag:

1. Virus
2. Information blir tillgänglig för obehöriga
3. Bristande kompetens
4. Integration
5. Användarnas kunskapsnivå

Det företag D har gjort för att förhindra dessa hot är att de har utarbetat ett regelverk för att få en styrning och ökad kompetens samt verktyg. De konsekvenser företag D skulle få om hoten skulle realiseras är att deras personsäkerhet kan vara i fara samt att deras förtroende även skulle minska hos personer som använder företaget.

Det är viktigt att göra riskanalyser för att ha kontroll på företagets säkerhet. Detta är något som även företag D gör och de gör det regelbundet, men även när direkta förändringar sker i företaget.

Företag E rangordnade följande fem hot som de största mot sitt företag:

1. Virus
2. Brand
3. Inbrott
4. Användarmisstag
5. -

De åtgärder som har gjort för att förhindra dessa hot är precis som många andra generellt brandväggar och andra säkerhetsåtgärder som finns inom branschen. De gör även backup på deras data varje dygn för att förhindra att information går förlorad.

Angående de konsekvenser som hade blivit om hoten genomförts skulle vara att kommunikationen skulle ha blivit väsentligt längre och svårare, faktureringen av kunder skulle även den försvåras och ta längre tid vilket skulle innebära att de fick likviditetsproblem på sikt. Deras kunder skulle också drabbas om avbrottet varade under en längre tid och kommunikationen med kunderna skulle då försvinna. Allt detta påverkar då statusen på företag E varumärke. Företag E har valt att endast göra sina riskanalyser vart annat år.

Företag F rangordnade följande fem hot som de största mot sitt företag:

1. Virus
2. Intrångsförsök
3. Insider
4. Ouppdaterad hårdvarumiljö
5. Ouppdaterad mjukvarumiljö

Företag F har precis som företag A dagliga uppdateringar av antivirusprogrammen på alla anställdas datorer. De har även policys för vilka program som får installeras på datorerna samt vilka webbplatser som inte får besökas.

Angående vilka konsekvenser olika hot kan orsaka är det mest att deras information kan läcka ut till obehöriga i och med detta, vilket de givetvis inte vill utsättas för. Företag F gör även de analyser av säkerheten i företaget och detta sker med ojämna intervaller.

4.2. Personer som säkerhetsrisker

Praktikanter och konsulter är vanligt förekommande hos företag och de kan i sig innebära en säkerhetsrisk. Företag A har satt upp regler att de inte får arbeta ensamma på kvällar eller helger för att ha kontroll på vad de gör. I övrigt gällande konsulter finns det regler med mera i avtal som gäller när de anlitar konsulter för att utföra ett arbete.

Företag A valde att inte svara på frågan om hur de hanterade insiders på företaget, av vilken anledning framgick inte.

Det händer att anställda på företaget gör misstag som kan påverka informationssäkerheten som att de kopplar in switchar och därmed stör nätet vilket företag A hade ändrat för att undvika. De tar även upp att ibland stör deras testsystem företagetsnätverk fast det inte ska det pga. misstag vilket då kan leda till att det överbelastas.

Företag B har dokumenterade rutiner angående hur de ska göra om en insider upptäcks på företaget. De rapporteras även direkt till säkerhetschefen om det misstänks att någon agerar insider på företaget.

När det gäller praktikanter på företag B har de som rutin att de inte får ha tillgång till känslig data eller till medarbetares konton till systemen. Medan de med konsulter gör upp ett sekretessavtal som de får skriva under samt att det ingår ett avtal som reglerar skadeståndsskyldighet ifall de ställer till med något.

Att anställda gör misstag som påverkar informationssystemet är något som är ganska vanligt på företag B. Det kan vara att anställda lämnar ut inloggningsuppgifter via phishing attacker eller att de helt enkelt glömmer logga ut från sitt konto när de lämnar datorn. En del anställda delar även lösenord med andra och familjemedlemmar, speciellt när det gäller trådlösa nätverk. De anställda som har en dator hemma som tillhör företaget låter andra familjemedlemmar använda den till privatbruk. Det är extra farligt om de är mobila dvs. bärbara datorer eller USB-stickor som de anställda sedan tar med till arbetsplatsen och kopplar in i datorerna där eller i nätverket och därmed kan smitta systemet.

Företag D har inga specifika rutiner angående hur de ska hantera insiders på företaget. Men när det gäller praktikanter och konsulter har de som regel att de måste inordnas under en ansvarig chef innan de får någon tillgång till deras nätverk och andra systemresurser.

Det sker även misstag av anställda på företag D som att persondata skickas till fel adress eller att data lämnas kvar på skärmen när den anställde lämnat datorn. Företag D har precis som företag B problem med att anställda tar med en USB-sticka hemifrån som de sedan ansluter till företag D nätverk och på detta vis då drar med sig virus in i systemet eller annan skadlig kod.

Angående hur företag E hanterar insiders på företaget vill de inte gå in på närmare än att de just har regler för hur de ska hantera insiders.

Även företag E ser praktikanter och konsulter som ett säkerhetsproblem mot deras informationssäkerhet. För att minimera denna risk har de som regel att de praktikanter och konsulter som ska arbeta för dem måste skriva på ett sekretessavtal beroende på vilket uppdrag de har.

När det gäller misstag som anställda gör på företaget vill inte företag E gå in närmare på än att det sker då de har valt att ha detta under sekretess.

De rutiner som Företag F har angående hanteringen av insiders är att ha reglering av detta i anställningsavtalen som då gäller spridning av företagets information med mera.

Företag F ser inte någon större risk med att ha praktikanter eller konsulter utan har istället val att ha ett stort förtroende för alla anställda på företaget och har en öppen miljö för alla. De har dock olika säkerhetsklassad information som de då styr via olika behörighetsnivåer.

Enligt företag F sker misstag på alla företag i mer eller mindre utsträckning och de tycker det viktigaste är att försöka förebygga dessa samt att agera på ett bra och effektivt sätt när de väl sker.

4.3. Utbildning och information om hot till anställda

När det gäller utbildning av anställda angående hot som finns mot informationssystem som t.ex. malware svarade företag A att de inte har någon speciell utbildning inom detta. De har bara lite utbildning av de anställda som arbetar med informationssäkerheten. Varför de övriga anställda inte får någon utbildning inom detta av något slag kunde de inte svara på.

Information om en hotbild ges dock ut till de anställda via nätet och om det inte är möjligt sker det istället muntligt direkt till de berörda eller så sätts anslag upp av lokala kontaktpersoner.

Företag B har ingen utbildning för sina anställda angående hot utan det är bara få anställda som arbetar med säkerhetsfaktorer som utbildas ibland. Varför de inte utbildar de övriga anställda beror det helt enkelt på ekonomin.

Även företag B skickar ut information när det finns en hotbild till de anställda. När det gäller hot mot den enskilda medarbetaren som t.ex. vid phishing attacker skickas det ut till alla anställda via e-mail. Medan när det gäller patcher för program med mera kontaktas endast IT-samordnarna. Ett problem de ser med detta att skicka ut information om hot är vad de kallar för ”vargen kommer syndromet”. Det innebär att om det skickas ut information för ofta kommer folk att strunta i att läsa det. Det samma gäller även antivirusprogrammen och brandväggen om det frågar för mycket klickar de till slut bara utan att se eller tänka efter vad det är.

Företag C däremot har valt att ha utbildning av de anställda angående hot som de kan utsättas för i något som de kallar CBT, computer based training. Även de skickar ut information om de har en hotbild mot sig till de anställda via e-mail, hemsidan eller muntligt. De anser att det finns en del risker med att skicka ut information angående hot men att det ändå väger över så pass mycket till det positiva att de inte ser nått större problem med det.

Företag D har inte heller dem utbildning av sina anställda och orsaken till detta ska vara att de helt enkelt inte hunnit dit än i sitt säkerhetsarbete.

De har valt att ha en krishanteringsplan och en kommunikationsplan som de tillämpar när det finns en hotbild mot dem. De för ut informationen till de berörda bland annat via hemsidan. Ett problem som företag D ser med att föra ut information angående hot är som de säger ”man får inte ropa vargen kommer i onödan”.

Företag E har inte de heller någon form av utbildning av sina anställda angående hot. De har inte sett något behov av att ha det, inte fram tills idag i alla fall. Angående hur de för ut information till de anställda om potentiella hot görs detta endast via mail. De ser heller inga problem med att göra detta utan är endast positiva till det.

Företag F har en sorts utbildning angående hot, det sker via information från deras infrastrukturavdelning och detta sker med jämna mellanrum.

Via mail och sms för företag F ut information om hotbilder som de ställs mot till de anställda. De ser inga problem med att skicka ut information om detta men de poängterar att det gäller att vara observant som anställd att kontrollera att mailet kommer från företaget. Det finns många sådana här utskick som är falska för att lura användare.

4.4. Regler och restriktioner för anställda

Något som i princip alla företag har är Internet och då det finns många faror på Internet så bör de ha regler. Detta är även något som företag A har, de har en företagspolicy där regler finns för de anställda om vad som får göras och inte göras. Det är i princip förbjudet att använda

Internet på företaget för privat bruk, men då det i dagens samhälle används ofta i kommunikation så tillåter de det till en viss mån. De ser helt enkelt lite mellan fingrarna på detta så länge ingen missbrukar det, sunt förnuft alltså.

Lösenord är något som alla anställda måste ha för att komma in i system med mera. Företag A har regler som lösenordsinterfacet styr angående valet av lösenord för de anställda. Det finns rekommendationer för hur ett lösenord ska se ut för att vara svårt att knäcka.

Många anställda har mobila enheter i sitt arbete vilket innebär en risk för företagen. Det har de även på företag A och de har satt upp specifika regler och vad de bör tänka på angående dessa med. Här under kommer några av dem:

- Avslöja aldrig ditt lösenord
- Öppna aldrig e-mail från okända avsändare
- Se till att antivirusprogrammet fungerar som det ska
- Kryptera alla konfidentiella bifogade filer
- Klassificera och skydda dina dokument
- Använd endast Internet för jobbrelaterade uppgifter
- Installera aldrig programvara utan tillstånd
- Rapportera alla brott mot informationssäkerheten till din närmaste chef
- Tänk på att det är fler som kan höra vad du säger vid samtal i mobiltelefonen på offentliga platser.
- Håll ett öga på datorn när du reser

Företag B har inga regler för Internetanvändning alls utan det enda de har är att när alla användare får ett konto skriver de på ett kontrakt som är mer på en etikett nivå. När det gäller regler för hur användarnas lösenord ska se ut har de krav på längd och komplexitet som måste följas. De har även en lösenordsgenerator till förfogande till dem som har dålig fantasi.

Även på företag B har anställda tillgång till mobila enheter i sitt arbete utefter det behov de har i sitt arbete. Men de har inga specifika regler angående mobila enheter utan det är bara de regler som gäller för fasta datorer och övrig resursanvändning som finns att tillgå även där.

Företag C förlitar sig mest till regeln använd med sunt förnuft när det kommer till Internetanvändningen på företaget. De har dock även valt att blockera vissa typer av kategorier på webben.

Företag D har regler angående Internetanvändning på företaget och de hänvisar till sin informationssäkerhetshandbok angående detta.

De anställda på företag D kan fritt välja sina lösenord till de olika systemen och datorerna. Men företaget har som mål att bli av med lösenord för att ersätta dessa med stark autentisering och ett identifieringskort.

På företag D har anställda tillgång till mobila enheter men endast enligt beslut av respektive chef. För att få ha detta måste de även ha en säker dator och ha en starkt autentisering. För att få mer information om regler angående detta hänvisar de till informationssäkerhetshandboken de har.

Hos företag E fanns inga specifika regler för Internetanvändning utan de tillämpar ”sunt förnuft”. Som att de sidorna de anställda surfar på skall vara arbetsrelaterade på något vis eller omvärldsbevakande samt att de inte får besöka sidor som är klassade som våld med mera.

Angående hur lösenord väljs av de anställda på företag E är detta valfritt men det finns vissa rekommendationer på hur ett lösenord ska konstrueras.

De anställda på företag E har tillgång till mobila enheter och de har även olika säkerhetsföreskrifter på hur en mobil enhet skall användas. Det finns ett dokument som innehåller information hur de anställda ska och får använda dem i kommunikation och användande för att säkerheten ska motsvara företagets krav.

Företag F har policys som hanterar vilka webbplatser som får besökas på nätet samt vilka typer av program som får installeras på deras datorer. De har även som några av de andra företagen fritt angående val av lösenord dock måste de följa ett visst regelverk som de har satt för lösenord. Alla anställda på företaget har även tillgång till mobila enheter och i deras fall är det endast mobiltelefoner.

5. Analys och diskussion

5.1. Hot mot företagets informationssystem

IT är ett område som växt något enormt de senaste åren. Det är en bransch som är under konstant utveckling och det släpps ofta nya produkter. Nu har i princip alla företag datorer och Internetuppkoppling att tillgå, som används i arbetet av de anställda. Men då det hela tiden kommer nya enheter och program som tas in och används på företagen innebär detta också att de utsätter informationssystemet för fler hot. Som det tas upp om i litteraturen (Kap 2.1.) fungerar inte dagens företag utan ett fungerande informationssystem, vilket leder till att verksamheten står still och det innebär kostnader för företaget.

Därför tänkte jag att det kunde vara intressant och undersöka vilka de största hoten mot ett företags informationssystem är just nu. Det är självklart att detta är en fråga där svaret konstant ändras i takt med utvecklingen inom IT och det spelar säkert in vilken typ av företag det är samt vilken storlek det är på företaget. Men jag anser ändå att detta område är väldigt intressant, då mycket av den litteratur som finns att tillgå mest innehåller diverse hot som finns mot företagens informationssystem och inte vilka som faktiskt utgör ett stort hot mot dem.

Denna typ av undersökning kan vara svår att göra då det ofta anses vara en känslig fråga hos företagen. De vill inte att information om vilka deras största hot är och hur de ska agera mot dem ska komma ut till personer som kan dra nytta av dem för att sedan använda det mot företaget. Därför var jag tydlig med att påpeka att de svarade helt anonymt på mina frågor dvs. att deras svar inte skulle gå att koppla till deras företag. Trots detta var det svårt att få företag att delta i undersökningen. Ett företag svarade t.ex. mestadels att det var sekretess på frågorna och svarade bara på enstaka frågor, medan ett annat företag svarade att de bara kunde ge ut denna typ av information till personer som de känt under en tid och därmed kunde lita på. Det kan diskuteras vilka andledningarna är till varför de inte vill delta om det beror på att de har en väldigt hög säkerhet med hårda regler eller att de inte har någon bra informationssäkerhet och därmed känner sig osäkra på att lämna ut information.

I undersökningen har företagen rangordnat sina topp fem hot mot företagens informationssystem och de visar på en del likheter. Ett hot som finns på alla företagens listor är virus, vilket i sig kanske inte är så konstigt då det är ett vanligt problem. Men det som är intressant med detta är att fyra av fem företag har satt virus som nummer ett på deras lista dvs. att det är deras största hot.

Virus är som nämnt i litteraturgenomgången (Kap 2.2.1.) den mest klassiska typen av malware attack. Den har funnits under många år och har ökat i farlighet i takt med att Internet växt. Det finns flera olika typer av virus och de är väldigt vanliga nu pga. Internet som bidrar stort i spridningen av dem. Virus kan göra en väldigt stor skada på ett företag rent informationsmässigt och driftmässigt, det var precis det som företag D fick uppleva när de fick in ett virus i deras informationssystem. Detta virus ledde till kostnader på 5 miljoner kronor för företag D. Då virus är en sådan vanlig företeelse på Internet är det inte speciellt

konstigt att den finns bland företagens topp fem hot då alla företag har Internet på sina företag idag.

Enligt Lundblad (2005) blir företagen allt mer mobila när det gäller var anställda arbetar någonstans och att det då är viktigt att ha specifika åtgärder mot hot för dessa. I undersökningen framkom att företagen hade anställda som använde sig av mobila enheter i arbetet.

Bärbara datorer är något som är vanligt förekommande på företag för att de anställda ska kunna arbeta på resande fot. De är en sårbarhet mot företagens informationssystem som nämns i litteraturgenomgången (Kap 2.6.). Problemet med dem är att de just är väldigt portabla, vilket innebär att användaren konstant måste ha kontroll över dem fysiskt men även ha viktig information krypterad. Det underlättar inte heller att sådana här enheter blir mindre och mindre vilket innebär att de lättare kommer bort. Något som är anmärkningsvärt gällande bärbara datorer är att personer kan lämna sin uppsyn över dem på t.ex. caféer och tåg när de uträttar något ärende. Jag tror att de inte tänker så mycket på den informationsmässiga förlusten som det blir om den blir stulen utan endast den materiella och det är därför de vågar göra detta.

5.2. Personer som säkerhetsrisker

Ett väldigt stort hot mot företagens informationssysten är deras egna anställda. De kan utgöra ett hot pga. deras okunskap eller att de gör rena misstag som kan skada informationssystemet på ett eller annat sätt.

Misstagsrelaterade eller olycksrelaterade hot var också vanligt förekommande i företagens listor. Detta med misstag kan relateras till den bristande kunskap och bristande kompetensen hos användare samt anställda som fanns i någons lista. Med detta menar jag att den bristande kunskapen kan leda till att de just gör misstag som de kanske inte hade gjort om de hade haft bättre kunskap inom området.

Anställda kan även vara ett hot i form av insider som det beskrivs om i litteraturen (Kap 2.3.). En del av företagen vill inte kommentera hur de går tillväga när en insider upptäcks medan andra hade specifika rutiner för det. Det är som företag F lite är inne på att det kan regleras i samband med anställningsavtalen. Detta stämmer överens bra med litteraturen (Kap 2.3.) där det skrivs att det är lite av en personalfråga dvs. hur rekryteringen går till och hur den anställde lämnar organisationen.

Det är vanligt att säga att det inte finns någon säker programvara, men det går också att säga att det inte heller finns några säkra användare. Användare kan medvetet, genom slarv eller ren okunskap göra fel som inga program i världen klarar av att hantera och därmed skada systemet. Det kan sägas att ett program är lika säkert som dess användare.

De åtgärder som företagen har gjort för att hindra att hoten realiseras har även de sina likheter. Nästan alla företagen har skrivit in antivirusprogram och brandväggar som ska hållas uppdaterat, precis som det nämnts om i litteraturgenomgången. De tar även upp saker som dagliga backuper, olika regelverk och policys angående vilka program som får installeras samt vilka webbplatser som får besökas, att nättrafiken övervakas och loggas. Men det som är mest intressant är att företag A har valt att hyra in ett externt företag som bemannar deras

reception. Varför de har valt att göra det visar på att de vill stärka säkerheten in till byggnaden, det externa företaget håller hårdare i reglerna än om det skulle stå egna anställda där. Det finns inte samma risk för att kollegor som man kommer bra överens med slinker ut med något eller att vänner lättare kommer in. Säkerheten blir mer skärpt med ett externt säkerhetsföretag. Möjligheten att upptäcka insiders blir även den större då de ser på de anställda från ett annat perspektiv än vad de egna anställda gör. Det kommer även att försvåra möjligheterna för en attackerare att ta sig in genom att använda sig av en social engineering attack som tailgating som presenterades i Kap 2.4.

5.3. Utbildning och information om hot till anställda

Det är egentligen konstigt att företagen inte satsar mer på att utbilda sin personal angående informationssäkerhet för att minska riskerna. Av de tillfrågade hade bara två av sex någon form av utbildning. Sen är frågan om alla får ta del av denna typ av utbildning eller om detta endast gäller de som arbetar med säkerheten. Det är ju den stora massan av anställda som utgör det största hotet och det är även dem man helst bör nå ut till. Detta är naturligtvis en kostnadsfråga som något företag nämner, då det kostar en hel del pengar att ha någon form av utbildning. Frågan är dock om de inte hade sparat pengar på att ha utbildning om företaget ser till de kostnader som det blir pga. misstag som görs beroende på bristande kunskap. Det är bara att se på exemplet som tidigare nämnts med företag D som fick ett virus, kanske hade detta gått att förhindra med utbildning av de anställda? De som arbetar med informationssäkerhet på företaget får även ett lättare arbete då och slipper åtgärda de anställdas datorer när de öppnat en fil i ett mail med ett virus i som infekterat datorn och gjort den obrukbar. Detta problem är något som det också tas upp om i InfoSäkerhetsutredningen (2004) att användare står för många olyckor och misstag som kan vara svåra att hindra. Det går inte att komma helt ifrån detta men det går säkerligen att minska problemet och om det väl inträffar bör de anställda vara informerade hur de ska agera när väl ett misstag eller en olycka inträffat. Problemet är att företag inte anser det vara nödvändigt med sådana här utgifter som det blir, utan tar hellre kostnaden sen när något inträffar.

Alla företagen skickade ut information till de anställda när det finns en hotbild mot dem. Detta kan vara en bra lösning när ens företag utsätts för t.ex. phishing mail som det togs upp om i litteraturgenomgången (Kap 2.4.2.). Där attackerare försöker lura av användare dess lösenord eller vad det nu kan vara. Genom att då skicka ut information om detta phishing mailet och att de inte ska klicka på det kommer det säkerligen göra att inga eller färre gör det. Två företag tar upp det här med vargen kommer syndromet, vilket innebär att de inte ska varna för vargen (hotet) hela tiden då de inte vet om den ens kommer. Det finns risk att användare som meddelas kommer sluta att ta dem på allvar och därmed sluta läsa dem. Men det är precis som företagen säger att fördelarna med att skicka ut information direkt när det finns en hotbild väger över de nackdelarna som finns med det. Ett annat problem kan vara att anställda kanske inte förstår informationen helt eller vilka konsekvenser det kommer bli om hotet realiseras. Även detta problem skulle kunna lösas med lite utbildning, för förstår de vilken skada ett hot kan göra kommer de säkerligen ta hotbilden på ett större allvar.

Det vanligaste sättet att föra ut sådan här information är via mail då det är oftast det sättet företaget kommunicerar med dess anställda samt att det är vid datorn säkerhetsrisken finns. Det finns en risk med att föra ut information av denna typ via mail och det är att en anställd kan missa mailet i den uppsjö av mail som vissa får. Ett företag skickade även ut information

angående hot via sms vilket är intressant då mobila enheter som smartphones även de utsätts för specifika attacker som det kan vara bra att informera om.

Det är intressant att ett företag skrev utbildning som en åtgärd mot hoten. Det kan tolkas som de är ett steg längre än de andra även om det är svårt att veta då de svarade sekretess på mycket. Men det är ändå värt att begrunda eftersom företaget är det enda som verkligen ser det som en lösning till de problem de utsätts för i och med dessa hot. Det är en lösning som inte syns då det varken är en mjukvarulösning eller en hådvarulösning men kan ändå vara lika effektiv.

5.4. Regler och restriktioner för anställda

Internet är något som finns på alla företag och idag används det till allt möjligt. Många använder det utöver i sitt arbete till att hålla kontakten med sina bekanta eller läsa nyheter på de olika nyhetssidorna som finns på webben med mera. De flesta företagen hade några få regler angående Internetanvändningen men de tillämpade egentligen regeln ”sunt förnuft”, vilket innebär att det är upp till användarna att avgöra vad som är rätt och fel. Detta är något som skiljer sig en del från person till person och det kan i slutändan ställa till med problem. En del kanske anser att det är okej att ladda ner små spel och spela dem på sin lunch eller fika. Det finns alltid en risk att spelfilen kan innehålla ett virus som kan infektera ens system när användaren startar det. Många anställda sitter och surfar på sociala medier under sin arbetstid som facebook. Det många inte tänker på när de gör detta är att det faktiskt finns många attackerare som just utnyttjar detta genom att ladda upp filer med skadlig kod eller helt enkelt lurar människor att lämna ut information eller liknande. Då olika personer har olika värderingar och har olika åsikter om vad som är rätt och fel kan detta i slutändan leda till att informationssystemet utsätts för risker som företaget kanske inte är beredd på.

Lösenord är något som alla anställda har och i takt med utvecklingen av teknik behövs det allt mer komplicerade lösenord för att de inte ska knäckas. Därför är det viktigt att ha regler för hur de ska se ut och hur långa de är precis som de företagen jag tillfrågade hade. Men fortfarande fick ändå användaren själva välja lösenord vilket i sig kan vara bra då de lättare kommer ihåg det. Men det många har för vana är att använda samma lösenord på flera ställen så knäcks det på ett ställe kan de komma in på andra ställen också. Om de anställda har dålig fantasi kan de använda sig av lösenordsgeneratorer för att slumpa fram ett bra och säkert lösenord. Detta kan bidra till att det är svårare att lära sig lösenordet utantill och att de anställda då istället väljer att skriva ner det för att sedan lägga det någonstans. Ett klassiskt ställe att placera sitt lösenord på är under tangentbordet. Det man då blir sårbar mot som nämns i litteraturen (Kap 2.4.) är desktop hacking. Där attackeraren letar igenom någons kontor för att just finna lösenordslappar. Eller om en anställd skulle slänga sitt lösenord i en papperskorg kan en attackerare även där använda sig av en social engineering attack som dumpster diving som beskrivs i litteraturen (Kap 2.4.) och på så sätt få tag i lösenordet. Detta är ju självklart inte bra för hittar någon detta kan de ta sig in i systemen och komma åt känslig information eller bara förstöra. Därför är det viktigt att ha dem i minnet istället och om användaren mot förmodan skulle glömma får de gå till IT-supporten på företaget och få ut ett nytt.

Något som är vanligt är att användare väljer lösenord som är riktiga ord dvs. ord som finns i en ordbok. Det innebär att ett ord som är långt som de anser är säkert i själva verket inte är det då de kan knäckas i en dictionary attack relativt snabbt. Detta är förmodligen något som

många normalanvändare inte vet om utan de tänker bara på lösenordets längd. Detta är något som kan förhindras genom att ge ut specifika lösenord som innehåller bokstäver, siffror och tecken som inte bildar något speciellt ord. Visst blir det svårare att lära sig lösenordet men om användaren skriver ett lösenord många gånger så lär de sig det oftast fort även om det ser komplicerat ut.

I undersökningen framkom att de tillfrågade företagen hade anställda som använde sig av mobila enheter i arbetet Men av dessa företag hade bara fyra regler eller information om vad de skulle tänka på specifikt för mobila enheter, medan ett företag inte hade något utöver de vanliga datorreglerna och ett inte hade något alls. Problemet med mobila enheter är att de kan vara svåra att skydda och att regler för dem ofta förbises samt att de kan enkelt bli fysiskt stulna. Därför är det viktigt att ha bra regler för dem så att inte viktig information läcker ut. Det är därför lite förvånande att alla företagen inte har några specifika regler för just mobila enheter, men att de ändå kan se flera olika problem och hot med dem. Som det tas upp om i litteraturen (Kap 2.6.) har många numer smartphones där de kan lagra alla möjliga sorters information om företaget. Då de har tillgång till mail och de kan lagra information direkt på den samt att de kan surfa på webben med den vilket innebär att de kanske loggar in på företagets webbsida. Dessa smartphones är därför utsatta för flera hot och de har generellt ganska dålig säkerhet i sig. Detta gör det än viktigare för företag att ha regler och anvisningar hur de ska hantera sina mobila enheter.

När det gäller hot mot informationssäkerheten på företag får man inte glömma bort de fysiska hoten som inbrott och brand. Det är hot som även dessa finns med på några av företagens listor över deras hot. Detta är något som många företag har bra åtgärder mot men det finns alltid en risk samt att vissa företag är mer utsatta än andra. Det är viktigt att ha klara rutiner för hur anställda ska agera och vad som ska ske vid en brand för att undvika stora skador som det tas upp om i litteraturen (Kap 2.5.). Att försvara sig mot en brand när det gäller att säkra informationen kan detta vara svårt om en byggnad drabbas så pass hårt att den brinner ner. För att då kommer förmodligen hårdvaran som informationen ligger lagrad på att förstöras helt och därmed försvinner även informationen. Det kan därför vara bra att ha backup på viktig information på ytligare en plats för att inte utsätta sig för risken att bli av med all sin information.

6. Slutsats

När forskningsfrågorna studerats och faktaunderlaget analyserats har följande resultat erhållits:

De största hoten mot ett företags informationssystem är främst malware hot, speciellt då virus samt misstags och olycksrelaterade hot. Av de företag som deltog i studien svarade alla att virus var på deras topp fem listor över hot mot deras informationssystem och alla utom ett rankade även det som det största hotet.

Den skada som hoten kan ha på företagen om hoten utlöses är att verksamhetens drift kan störas, deras kunder kan drabbas, varumärkets status kan ta skada, ekonomiska konsekvenser och att företagshemligheter kan läcka ut. Detta kan leda till att verksamheten står still och därmed får projekt att stanna upp, även konkurrenter kan få reda på deras företagshemligheter om de läcker ut och allt detta kan leda till stora kostnader för företaget. Det var precis detta som ett av företagen i studien fick uppleva när det drabbades av ett virus.

Den möjlighet företagen har att skydda sig mot de olika hoten var främst de klassiska åtgärder som antivirusprogram, brandväggar, loggning över nättrafik, backuper och att hålla alla program uppdaterade med den senaste uppdateringen av programvaran. Det fanns även andra mer specifika åtgärder beskrivna som att ha externt bemannad reception för att öka den fysiska säkerheten. Den åtgärd som var mest intressant var de som svarade utbildning, det visar att det finns de som förstår att deras egna anställda kan utgöra ett stort hot mot det egna företaget och att de är villiga att utbilda dem för att minimera denna risk.

Vem eller vad kan vara orsak till hoten. När det gäller hot som malware är det oftast en attackerare som har som orsak att skada något eller någon. Men det behövs även någon som får in viruset på företagets system och om resultaten tolkas angående de anställdas misstag kan det ses en koppling mellan detta. Det är nämligen så att det är de anställda själva som drar in virus genom att klicka på länkar i mail eller får med sig det hemifrån genom USB-stickor med mera. Den reflektion som kan göras är att det är någon illasinnad attackerare som oftast skapar hotet medan det är den anställde som realiserar det.

Analysen av undersökningen, som genomfördes med ett frågeformulär, och teoriunderlaget identifierade samt gav kunskap om de största hoten mot ett företags informationssystem vilket var syftet med studien.

6.1. Fortsatt forskning

När det gäller fortsatt forskning inom detta ämne kan det vara intressant att göra en större undersökning dvs. att fler företag ingår i undersökningen. För att se om det blir liknande resultat med fler tillfrågade företag. Det kan även vara intressant att tillfråga olika branscher,

olika företagsstorlekar och ägarförhållanden för att se om det uppstår skillnader mellan dem i informationssäkerheten på företagen.

Något som skulle vara intressant att göra en fortsatt studie på är de anställdas kunskaper angående de olika hoten som ett företags informationssystem kan utsättas för. Att undersöka hur mycket den ”vanlige” anställde vet om informationssäkerhet för att kunna styrka än mer på att det är en viktig punkt angående säkerheten på företag. Detta kan vara väldigt intressant att se hur de anställda ligger till rent kunskapsmässigt då många av företagen hävda att det gjordes en hel del misstag som kan kopplas till de anställdas kunskap.

Bilagor

B1 Frågeformulär

- Vilka hot har ni mot företagets informationssystem (rangordna de fem största och motivera varför)?
    - Vilka åtgärder har gjorts för att hantera dessa hot?
    - Vilka konsekvenser skulle det ha fått om hotet genomförts?
- Gör företaget analyser av säkerhetsrisker regelbundet och i så fall hur ofta?
- Hur hanterar ni det här med insiders på företaget (finns det några rutiner osv.)?
- Ses praktikanter och konsulter som säkerhetsrisker? Har ni specifika regler för dem?
- Händer det att anställda gör misstag som kan påverka informationssäkerheten (vilken typ av misstag kan förekomma)?
- Har ni någon form av utbildning av de anställda angående hot som t.ex. malware och social engineering?
    - Om ja, sker det löpande eller hur har ni det?
    - Vid nej, motivera varför?
- För ni ut direkt information när det finns en hotbild mot informationssystemet till de anställda som berörs (via hemsidan, e-post, muntligt)?
- Kan ni se nackdelar eller risker med att gå ut med information om hot, så fall på vilket sätt?
- Finns det regler för Internetanvändning på företaget och hur ser de i så fall ut?
- Får de anställda välja egna lösenord fritt eller finns det specifika krav på dem?
    - Använder ni en lösenordsgenerator, om "nej", varför inte?
- Har anställda på företaget tillgång till mobila enheter i sitt jobb?
    - Finns det några säkerhetsföreskrifter angående mobila enheter?

B2 Företag A

Generellt kan nämnas att vår IS/IT-miljö sköts av ett externt företag.
Vår IS/IT-säkerhet styrs av vår säkerhetsansvarige inom Företag A som i sin tur ger direktiv till det externa företaget.

- Vilka hot har ni mot företagets informationssystem (rangordna de fem största och motivera varför)?

  Virusangrepp
  Intrång via nätet.
  Inbrott eller obehörig vistelse i våra lokaler.
  Användarmisstag. (t.ex. loop-kopplade switchar i konferensrum)
  Misstag från IS/IT-support.

  - Vilka åtgärder har gjorts för att hantera dessa hot?

  -Alla datorer utrustade med antivirusprogram och brandväggar. Uppdateras dagligen. On access hantering kompletterat med veckovis fullscanning.
  -Microsoft säkerhetspatchar installeras automatiskt.
  -Receptionen bemannad av externt säkerhetsföretag. Övriga säkerhetsdetaljer kan jag av naturliga skäl inte avslöja.
  -Jag tror switcharna bytts mot loop-säkra.

  - Vilka konsekvenser skulle det ha fått om hotet genomförts?

  Tillgång till företagshemligheter. Sabotage vilket kan medföra förseningar av projekt och ekonomiska konsekvenser.

- Gör företaget analyser av säkerhetsrisker regelbundet och i så fall hur ofta?

  Vi har en separat avdelnings om sysslar med detta. Lokalt gör vi årligen eller mer sällan riskanalys av vår egen utrustning dvs. utrustning som inte sköts av det externa IS/IT-företaget.

- Hur hanterar ni det här med insiders på företaget (finns det några rutiner osv.)?

- Ses praktikanter och konsulter som säkerhetsrisker? Har ni specifika regler för dem?

  Får inte jobba ensamma på kvällstider och helger. I övrigt är detta uppstyrt i avtalet med konsulterna.

- Händer det att anställda gör misstag som kan påverka informationssäkerheten (vilken typ av misstag kan förekomma)?

  -Se ovan om loop-koppling av switchar.
  - Våra testsystem skall vara isolerade från företagsnätverket men ibland sker misstag

vilket kan belasta nätet i onödan. Övervakas externt och stänger ner portar för att isolera problemet.

- Har ni någon form av utbildning av de anställda angående hot som t.ex. malware och social engineering?

  - Om ja, sker det löpande eller hur har ni det?

  Känner inte till begreppen även om jag delvis kan gissa vad det betyder. Ingen speciell utbildning mer än för IS/IT-personal.

  - Vid nej, motivera varför?

  Vet ej. Inte mitt bord.

- För ni ut direkt information när det finns en hotbild mot informationssystemet till de anställda som berörs (via hemsidan, e-post, muntligt)?

  Ja, i den mån det är möjligt. Om det inte går via nätet så sker det muntligen eller via anslag av lokala kontaktpersoner.

  - Kan ni se nackdelar eller risker med att gå ut med information om hot, så fall på vilket sätt?

  Vet ej.

- Finns det regler för Internetanvändning på företaget och hur ser de i så fall ut?

  Det finns en företagspolicy. I princip är det förbjudet att använda för privat bruk, men samtidigt är det en del av dagens kommunikationssätt så i viss mån ser man mellan fingrarna så länge det inte missbrukas. Sunt förnuft.

- Får de anställda välja egna lösenord fritt eller finns det specifika krav på dem?

  Lösenord väljs enligt de regler som lösenordsinterfacet styr upp. Rekommendationer finns.

  - Använder ni en lösenordsgenerator, om "nej", varför inte?

  Nej. Vet ej.

- Har anställda på företaget tillgång till mobila enheter i sitt jobb?

  Ja

  - Finns det några säkerhetsföreskrifter angående mobila enheter?

  Att tänka på……

  - *Avslöja aldrig ditt lösenord*

- *Öppna aldrig e-post från obekanta avsändare*
- *Se till att ditt virusprogram fungerar som det ska*
- *Kryptera alla konfidentiella bifogade filer*
- *Klassificera och skydda dina dokument*
- *Använd endast Internet för jobbrelaterade uppgifter*
- *Installera aldrig programvara på datorn utan tillstånd*
- *Rapportera alla brott mot informationssäkerheten till din närmaste chef*
- *Tänk på att det är fler som kan höra vad du säger vid samtal i mobiltelefon på offentlig plats*
- Håll ett öga på datorn när du reser

B3 Företag B

- Vilka hot har ni mot företagets informationssystem (rangordna de fem största och motivera varför)?

1 Att folk lämnar ut/sprider eller att trojaner eller liknande registrerar lösenord så att det går att komma åt känsliga data. Även avlyssning.
2 Försöka ta över maskiner (komma över lösen) till exempelvis ”pirat-ftp” sajt, ddos attacker etc.
3 Virus som slår ut datorer och/eller förstör data.
4 Diskkrascher och fel handhavande exempelvis förstör data. Att medarbetarna inte säkrar sina data är en stor riskfaktor.
5 Eftersom vi är spridda är systemstopp och nätfel en risk för verksamheten. Bristande redundans.

  - Vilka åtgärder har gjorts för att hantera dessa hot?

  Virusskydd och brandväggar lokalt på varje dator samt detsamma på alla servrar. Dessutom finns flera brandväggsnivåer i nätet.
  Kontinuerlig övervakning av nätet där system analyserar och letar efter ovanliga händelser.
  Loggning av all trafik inklusive mailtrafik (mot phishing tex).
  Filservrar skyddade genom att åtkomsten är hårt reglerad.
  Info till anställda.

  - Vilka konsekvenser skulle det ha fått om hotet genomförts?

  Säger sig självt.

- Gör företaget analyser av säkerhetsrisker regelbundet och i så fall hur ofta?

Vet ej. Ligger på säkerhetschefen.

- Hur hanterar ni det här med insiders på företaget (finns det några rutiner osv.)?

Det finns dokumenterade rutiner. Misstankar bollas upp till säkerhetschefen.

- Ses praktikanter och konsulter som säkerhetsrisker? Har ni specifika regler för dem?

Praktikanter får inte åtkomst till ”känsliga data” eller medarbetarnas konton.
Konsulter skriver under sekretessavtal samt ingår ett avtal som reglerar skadeståndsskyldighet i fall de ställer till något.

- Händer det att anställda gör misstag som kan påverka informationssäkerheten (vilken typ av misstag kan förekomma)?

Ja tyvärr. Lämnar ut inloggningsuppgifter t.ex. vid phishing. Glömmer att logga ut. Delar lösenord med andra och familjemedlemmar (speciellt gällande trådlösa nät). Låter

familjen utnyttja Företag B-datorer hemma och när det gäller mobila sedan tar med till jobbet och överför både det ena och det andra. USB-minnen som smittas.

- Har ni någon form av utbildning av de anställda angående hot som t.ex. malware och social engineering?

Nej.

  - Om ja, sker det löpande eller hur har ni det?

  Dock får de som sysslar med säkerhetsfaktorer viss utbildning ibland.

  - Vid nej, motivera varför?

  Ekonomin…..

- För ni ut direkt information när det finns en hotbild mot informationssystemet till de anställda som berörs (via hemsidan, e-post, muntligt)?

Ja genom e-post. När det gäller sådant som rör den enskilda medarbetaren t.ex. phishing går det ut till alla, när det gäller patchning etc. går det bara ut till IT-samordnarna.

- Kan ni se nackdelar eller risker med att gå ut med information om hot, så fall på vilket sätt?

”Vargen kommer syndromet”. Om man går ut för ofta struntar folk i det. Samma om t.ex. virusskyddet/brandväggen frågar för mycket klickar folk bort allt till sist utan att se vad det är.

- Finns det regler för Internetanvändning på företaget och hur ser de i så fall ut?

Nej. Finns dock ett kontrakt som alla som får ett konto undertecknar. Det är mer på en ”netikett” nivå.

- Får de anställda välja egna lösenord fritt eller finns det specifika krav på dem?

Ja enligt de krav på längd och komplexitet som finns.

  - Använder ni en lösenordsgenerator, om "nej", varför inte?

  Finns för de som har dålig fantasi, annars behövs det inte.

- Har anställda på företaget tillgång till mobila enheter i sitt jobb?

Ja efter behov i sitt arbete.

  - Finns det några säkerhetsföreskrifter angående mobila enheter?

  Inga utöver som gäller för de fasta datorerna och övrig resursanvändning.

B4 Företag C

- Vilka hot har ni mot företagets informationssystem (rangordna de fem största och motivera varför)?

Samma hot som alla andra. Integritetshot, avlyssning osv.

  - Vilka åtgärder har gjorts för att hantera dessa hot?

  Utbildning, bl.a övrigt lyder under sekretess.

  - Vilka konsekvenser skulle det ha fått om hotet genomförts?

  Sekretess

- Gör företaget analyser av säkerhetsrisker regelbundet och i så fall hur ofta?

Ja, Sekretess

- Hur hanterar ni det här med insiders på företaget (finns det några rutiner osv.)?

Sekretess

- Ses praktikanter och konsulter som säkerhetsrisker? Har ni specifika regler för dem?

Nej och Ja

- Händer det att anställda gör misstag som kan påverka informationssäkerheten (vilken typ av misstag kan förekomma)?

Ja, övrigt lyder under sekretess

- Har ni någon form av utbildning av de anställda angående hot som t.ex. malware och social engineering?

Ja

  - Om ja, sker det löpande eller hur har ni det?

  CBT, Computer based training

  - Vid nej, motivera varför?

- För ni ut direkt information när det finns en hotbild mot informationssystemet till de anställda som berörs (via hemsidan, e-post, muntligt)?

Ja, alla tre alternativ.

- Kan ni se nackdelar eller risker med att gå ut med information om hot, så fall på vilket sätt?

Finns vissa risker i ett fåtal fall. Dessa fall är i klar minoritet. Fördelarna är långt mycket större.

- Finns det regler för Internetanvändning på företaget och hur ser de i så fall ut?

Ja, använd med förnuft. Vissa kategorier är blockade.

- Får de anställda välja egna lösenord fritt eller finns det specifika krav på dem?

Specifika krav

  - Använder ni en lösenordsgenerator, om "nej", varför inte?

  Bra fråga, vet ej. Vi har inte haft behovet.

- Har anställda på företaget tillgång till mobila enheter i sitt jobb?

Ja

  - Finns det några säkerhetsföreskrifter angående mobila enheter?

  Jepp

B5 Företag D

- Vilka hot har ni mot företagets informationssystem (rangordna de fem största och motivera varför)?

1. Virus – vi har varit utsatta för ett virusangrepp som kostade mycket – ca 5 milj
2. Informationen kan bli tillgänglig för obehöriga – måste vara tillgänglig för patientsäkerheten men bara läsas av behöriga
3. Brist på kompetens – bla outsorcing
4. Integration – posistvt ur användarens synpunkt men risk att man skapar alltför komplex miljö
5. Användarnas kunskapsnivå

- Vilka åtgärder har gjorts för att hantera dessa hot?

Utarbetar regelverk för att få styrning, ökad kompetens och verktyg

- Vilka konsekvenser skulle det ha fått om hotet genomförts?

Kan vara fara för patientsäkerheten och minska förtroendet för Företag D hos invånare/patienter

- Gör företaget analyser av säkerhetsrisker regelbundet och i så fall hur ofta?

Riskanalyser ska genomföras regelbundet och vid förändringar

- Hur hanterar ni det här med insiders på företaget (finns det några rutiner osv.)?

Inga specifika rutiner

- Ses praktikanter och konsulter som säkerhetsrisker? Har ni specifika regler för dem?

Alla måste inordnas under ansvarig chef innan tillgång till nätverk och systemresurser.

- Händer det att anställda gör misstag som kan påverka informationssäkerheten (vilken typ av misstag kan förekomma)?

Ex. skickar fax eller mail med patientdata till fel adress, lämnar datorn på med patientinformation på skärmen, tar med ett USB-minne hemifrån med virus och ansluter till Företag D nätverk och på så sätt sprider virus eller annan skadlig kod.

- Har ni någon form av utbildning av de anställda angående hot som t.ex. malware och social engineering?

Nej

- Om ja, sker det löpande eller hur har ni det?

- Vid nej, motivera varför?

Har inte hunnit dit

- För ni ut direkt information när det finns en hotbild mot informationssystemet till de anställda som berörs (via hemsidan, e-post, muntligt)?

Finns krishanteringsplan och kommunikationsplan – förs ut via hemsida mm

- Kan ni se nackdelar eller risker med att gå ut med information om hot, så fall på vilket sätt?

Svårt att bedöma allvaret – man får inte ropa Vargen kommer i onödan

- Finns det regler för Internetanvändning på företaget och hur ser de i så fall ut?

Se informationssäkerhetshandboken

- Får de anställda välja egna lösenord fritt eller finns det specifika krav på dem?

Välja i princip fritt, mål att bli av med lösenord och ersätta med stark autentisering och ID-kort

- Använder ni en lösenordsgenerator, om "nej", varför inte?

- Har anställda på företaget tillgång till mobila enheter i sitt jobb?

Ja, enligt beslut av resp. chef , kräver säker dator och stark autentisering mm

- Finns det några säkerhetsföreskrifter angående mobila enheter?

Se informationssäkerhetshandboken

B6 Företag E

- Vilka hot har ni mot företagets informationssystem (rangordna de fem största och motivera varför)?

Virus
Brand
Inbrott
Användarmisstag

  - Vilka åtgärder har gjorts för att hantera dessa hot?

  Generellt brandväggar och andra säkerhetsåtgärder som används inom branschen
  Backup varje dygn

  - Vilka konsekvenser skulle det ha fått om hotet genomförts?

  Väsentligt längre och svårare kundkommunikation, fakturering av kund försvåras och tar tid vilket innebär likviditetsproblem på sikt
  Risk för väsentligt längre avbrott för våra kunder
  Varumärket påverkas då ingen kommunikation kan hanteras,
  Kommunikation med kunderna försvinner, ökade arbetsinsatser

- Gör företaget analyser av säkerhetsrisker regelbundet och i så fall hur ofta?

Ja vart annat år

- Hur hanterar ni det här med insiders på företaget (finns det några rutiner osv.)?

Ja det finns insiderregler

- Ses praktikanter och konsulter som säkerhetsrisker? Har ni specifika regler för dem?

Ja, de får skriva på sekretessavtal beroende på uppdrag

- Händer det att anställda gör misstag som kan påverka informationssäkerheten (vilken typ av misstag kan förekomma)?

Ja, men detta är sekretess, trots Företag 1 osv.

- Har ni någon form av utbildning av de anställda angående hot som t.ex. malware och social engineering?

Nej

  - Om ja, sker det löpande eller hur har ni det?

- Vid nej, motivera varför?

  Vi har inte sett det behovet fram till idag.

- För ni ut direkt information när det finns en hotbild mot informationssystemet till de anställda som berörs (via hemsidan, e-post, muntligt)?

Mail

- Kan ni se nackdelar eller risker med att gå ut med information om hot, så fall på vilket sätt?

Inga nackdelar

- Finns det regler för Internetanvändning på företaget och hur ser de i så fall ut?

I princip inte, det är sunt förnuft som gäller och surfandet skall vara arbetsrelaterat och omvärldsbevakande, men självklart är det inte tillåtet att vara på sidor som är klassificerade inom våld och andra liknande sektorer.

- Får de anställda välja egna lösenord fritt eller finns det specifika krav på dem?

Ja men det finns rekommendationer

- Använder ni en lösenordsgenerator, om "nej", varför inte?

- Har anställda på företaget tillgång till mobila enheter i sitt jobb?

Ja

- Finns det några säkerhetsföreskrifter angående mobila enheter?

  Ja, Det finns ett dokument som beskriver hur en mobil enhet skall och får användas för att kommunikation och användande skall ha en säkerhet som motsvarar våra krav.

B7 Företag F

- Vilka hot har ni mot företagets informationssystem (rangordna de fem största och motivera varför)?

(1) Virus
(2) Intrångsförsök
(3) Att någon lämnar information till konkurrenter
Att vi inte alltid hänger med i den snabba utvecklingen gällande våra egna miljöer, dvs. datorer (4) och senaste programvaran för operativ system/stödprogram etc.(5)

- Vilka åtgärder har gjorts för att hantera dessa hot?

Alla anställda har dagliga uppdateringar av antivirusprogram och policys för vilken typ av program och webbplatser som inte får installeras på våra datorer/besökas

- Vilka konsekvenser skulle det ha fått om hotet genomförts?

Det beror på vilken typ av ”angrepp” virus är ju alltid ett reellt hot, och vi vill inte att någon obehörig ska kunna komma åt vår information

- Gör företaget analyser av säkerhetsrisker regelbundet och i så fall hur ofta?

Ja. det sker med ojämna intervaller

- Hur hanterar ni det här med insiders på företaget (finns det några rutiner osv.)?

Reglering via anställningsavtal gällande spridning av information etc.

- Ses praktikanter och konsulter som säkerhetsrisker? Har ni specifika regler för dem?

Vi har stort förtroende för alla våra anställda och vi har en öppen miljö för alla, det finns även säkerhetsklassad information som styrs via behörigheter

- Händer det att anställda gör misstag som kan påverka informationssäkerheten (vilken typ av misstag kan förekomma)?

Misstag kan alla göra och det sker i varje företag, det viktiga är att förebygga och om något händer agera på ett effektiv sätt

- Har ni någon form av utbildning av de anställda angående hot som t.ex. malware och social engineering?

- Om ja, sker det löpande eller hur har ni det?

Det sker via information från vår infrastrukturavdelning med jämna mellanrum

- Vid nej, motivera varför?

- För ni ut direkt information när det finns en hotbild mot informationssystemet till de anställda som berörs (via hemsidan, e-post, muntligt)?

Ja, via mail/sms

- Kan ni se nackdelar eller risker med att gå ut med information om hot, så fall på vilket sätt?

Nej det är bättre att förebygga, men man kan ibland se spam som är förtäckta att komma från en ”IT-avdelning”, så detta får man vara observant på

- Finns det regler för Internetanvändning på företaget och hur ser de i så fall ut?

Vi har och policys för vilken typ av program och webbplatser som inte får installeras på våra datorer/besökas

- Får de anställda välja egna lösenord fritt eller finns det specifika krav på dem?

Valfritt men efter ett regelverk

- Använder ni en lösenordsgenerator, om "nej", varför inte?

  Jag kan inte svara på denna fråga!

- Har anställda på företaget tillgång till mobila enheter i sitt jobb?

Alla anställda har mobiler

- Finns det några säkerhetsföreskrifter angående mobila enheter?

  Jag kan inte svara på denna fråga!

Referenser

Ahmad, D. et al. (2002) Hack Proofing Your Network. 2 ed. Rockland: Syngress.

Anti Phishing Working Group (APWG) (2009) *Phishing Activity Trend Report Q4 2009*. [online] Anti-Phishing Working Group. Available from http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf [Accessed 18 maj 2010].

Arbetsmiljöverket. Hemsida [online] 2010 Tillgänglig: http://www.av.se/teman/datorarbete 2010-05-10

Aycock, J. (2006) *Computer Viruses and Malware*. Advances in Information. volume 22. Springer Science+Business Media, LLC

Baskin, B. & Piltzecker, T. (2006) *Combating spyware in the enterprise*. Burlington: Syngress.

Brandell, J. (2010) *McAfee – uppdateringen slog ut tiotusentals datorer.* IDG.se [online] 2010-04-22 Tillgänglig från http://www.idg.se/2.1085/1.312684/mcafee-uppdatering-slog-ut-tiotusentals-datorer [20 maj 2010]

Carlsson, B. (2007) *Hot och svek. Säkerhet hos människor och datorer*. Lund: Studentlitteratur.

Contos, B. (2006) *Enemy at the water cooler Real-life stories of insider threats and Enterprise Security Management countermeasures*. Burlington: Syngress.

Dubrawsky, I. (2007) *How to cheat at securing your network.* Burlington: Syngress.

Dunham, K. (2009) *Mobile malware attacks and defense*. Syngress/Elsevier.

Gollmann, D. (2006) *Computer Security*. 2. ed. West Sussex: John Wiley & Son Ltd.

InfoSäkerhetsutredningen (2004) *Informationssäkerhet i Sverige och internationellt. – översikt.* Stockholm : Fritzes. (Statens offentliga utredningar 2004:32).

Jacobsen, D. I. (2002) *Vad, hur och varför? Om metodval i företagsekonomi och andra samhällsvetensapliga ämne*. Upplaga 1:8. Lund: Studentlitteratur.

Josephson, H. (red). (2007) *Norstedts Uppslagsbok*. 14 uppdaterad och utök. Uppl. Stockholm: Norstedt.

Lagersten, J. (2009) *Utvärdera Informationssystem. Pragmatiskt perspektiv och metod.* Lindköping studies in Arts and science. No 489. Lindköping: Lindköpings universitet.

de Leeuw, K. (2007) *The history of information security. A comprehensive handbook.* Amsterdam: Elsevier B.V.

Lundblad, N. (2005) *Säkra ditt företag – Informationssäkerhet för chefer och ledare*. Malmö: Liber.

Mitnich, K.& Long, J. (2008) *No tech hacking A guide to social engineering, dumpster diving and shoulder surfing.* Syngress.

Myhr, B. et al. (2004) *Stäng fönstret för objudna gäster. – IT säkerhet för små företag*. Kista: Symantec Nordic AB.

Nohlberg, M. (2008) *Securing Information Assets: Understanding, Measuring and protecting against Social Engineering Attacks*, Diss. Stockholm: Stockholms universitet.

Pfleeger, C. P. & Pfleeger, S. L. (2003) *Security in Computing*. 3. ed. New Jersey: Pearson Education, Inc.

Pfleeger, S. L. et al. (2010) *Insiders Behaving Badly: Addressing Bad Actors and Their Actions* IEEE Transactions on Information Forensics and Security 5(1) pp 169-179.

Region Skåne. *Informationssäkerhetshandbok* [online] 2010-02-02 Tillgänglig: http://www.skane.se/templates/Page.aspx?id=45633 [2010-05-09]

Rienecker, L. & Jorgensen, P. S. (2008) *Att skriva en bra uppsats*. Upplaga 2. Malmö: Liber.

Stadgis, J. *13 hot att se upp med 2010*. Computer Sweden. [online] 2009-12-21. Tillgänglig från: http://www.idg.se/2.1085/1.280931/13-hot-att-se-upp-med-2010 [19 maj 2010]

Stallings, W. (2003) *Network Security Essentials. Applications and Standards*. 2. ed. New Jersey: Pearson Education, Inc.

Stewart, J. & James, L. (2005) *Phishing Exposed*. Rockland: Syngress.

Syrén, A. (2005) *På egen risk. En handbok om informationssäkerhet*. Stockholm: SIS förlag.

Örnborg, M. & Jacobsen, O. (2010) *Största IT-hoten mot svenska företag*. Metroteknik [online] 21-27 april 2010. s. 8. Tillgänglig från: http://www.metro.se/se/misc/pdf/2010/04/21/SETEK_2010_04_21.pdf [19 maj 2010]