Informationssäkerhet och mobila enheter

Basnivå för informationssäkerhet (BITS) och dess hantering av mobila enheter

Kandidatuppsats, 10 poäng, inom Systemvetenskapliga programmet

Framlagd: 06, 2006

Författare: Erik Forsberg
Frode Wikesjö

Handledare: Kjell Åke Holmberg

LUNDS UNIVERSITET
Informatik

Informationssäkerhet och mobila enheter

Basnivå för informationssäkerhet (BITS) och dess hantering av mobila enheter

© Erik Forsberg
Frode Wikesjö

Kandidatuppsats framlagd 06, 2006
Omfång: 50 sidor
Handledare: Kjell Åke Holmberg

Resumé

Mobila enheter såsom bärbara datorer, avancerade handdatorer och mobiltelefoner blir allt vanligare i organisationer. Tidigare har informationssäkerhet byggts upp för att skydda organisationer från attacker utifrån, men nu måste man även skydda organisationen inifrån. Detta för att enheter tas ut ur organisationen och utsätts för andra, möjligt farliga miljöer. För att sedan på nytt föras in i organisationens nätverk. Basnivå för informationssäkerhet, BITS är riktlinjer framtagna av Krisberedskapsmyndigheten. Riktlinjer för minsta acceptabla informationssäkerhetsnivå i organisationer. I uppsatsen undersöks hur BITS hanterar problem och hot som uppkommer vid användandet av mobila enheter. För att undersöka problemen genomfördes tre expertintervjuer, experterna var tre av Sveriges inom ämnet mest kunniga och meriterade individer. Resultatet av intervjuerna analyserades och jämfördes med BITS. Vår undersökning fann att BITS har brister i hur organisationer ska hantera mobila enheter och de risker och hot som finns i användandet av dessa. Bristerna fanns i att BITS inte framhåller att man ska använda så kallad lager-på-lager säkerhet.

Nyckelord
Informationssäkerhet, mobila enheter, Basnivå för informationsäkerhet, BITS

Innehållsförteckning

Figurförteckning

1 Inledning

Säkerhet relaterad till informationsteknik (IT) är ett högaktuellt ämne, alltmer av vårt dagliga liv påverkas på ett eller annat sätt av IT. I stora delar av världen blir vi mer beroende av att denna teknik fungerar. Enligt en undersökning genomförd av Statistiska Centralbyrån (SCB) använder 96% av företagen med tio eller fler anställda datorer i sitt arbete, vilket ger en indikation på hur beroende vi är av informationsteknik (Företagens användning av datorer och Internet, SCB, 2005).

Med bristande informationssäkerhet följer höga kostnader för organisationer, i en rapport från amerikanska Federal Bureau of Investigation (FBI) där IT-relaterade brott undersöktes fann de skrämmande siffror. FBI beräknar att den årliga kostnaden för IT-relaterade brott hos amerikanska företag är omkring 500 miljarder svenska kronor, samma rapport fann även att 64% av de tilltalade organisationerna hade förlorat pengar på denna typ av brott. Med IT-relaterade brott menas bland annat virus, maskar, datastölder och intrång (CSI, 2005).

Man kan tro att sårbarheterna i informationssystemet har minskat med åren, att vi lärt oss av det förgångna, men så är inte fallet. 2005 dokumenterade säkerhetsföretaget Symantec 40% mer sårbarheter i mjukvara jämfört med år 2004, vilket är en antydan på hur pass aktuellt ämnet är (Symantec Internet Security Threat Report, 2006).

Det faktum att vi använder allt mer mobila enheter såsom bärbara datorer, handdatorer, mobiltelefoner etc. ställer problematiken på högkant. Tidigare kunde man inom ett företag skydda sig från intrång utifrån och försäkra sig om att man hade en säker miljö internt. Nu tas enheterna ut från företagets domäner och dess kontroll, för att sedan föras in igen. Ett annat problem som uppkommer med användandet av mobila enheter är när de innehåller känslig information och blir stulna eller borttappade. Samtidigt kommer nya tekniker som trådlösa nätverk mer in i vår vardag, vilket också bidrar till en förändrad informationssäkerhetssituation.

1.1 Bakgrund

Vad är/menas således med informationssäkerhet? I SIS *Handbok i informationssäkerhetsarbete(2002)* definieras informationssäkerhet enligt SS-ISO/IEC 17799:2000 på följande sätt: ”*Information är en tillgång som, liksom andra viktiga tillgångar i en organisation, har ett värde för en organisation och följaktligen få ett lämpligt skydd. Informationssäkerhet syftar till att skydda information mot en mängd olika hot för att säkerställa verksamhetens kontinuitet, minska skador på verksamheten och maximera avkastningen på investerat kapital samt affärsmöjligheter*”

Lenander (1998) anser att informationssäkerhet är ett samlingsbegrepp för all säkerhet som har anknytning till hur information hanteras. Detta gäller både för information som hanteras manuellt och med hjälp av datorer. Man kan enligt honom dela upp informationssäkerhet i två delar, IT-säkerhet och administrativ säkerhet. Där IT-säkerheten hanterar informationen som bearbetas, lagras eller skickas mellan olika datorer, medan den administrativa säkerheten hanterar

säkerhetsfrågor angående information som bearbetas manuellt. Statskontoret (1997) är av åsikten att informationssäkerhet inkluderar både traditionell datasäkerhet och säkerhet som är relaterad till hantering av information i olika verksamheter. Eftersom informationssäkerhet är en integrerad del i ett informationssystem anser Ledell (1991) att det är självklart att det i ett datoriserat informationssystem krävs informationssäkerhet.

Information är en otroligt viktig beståndsdel för organisationer och deras existens, information som finns inom företagen måste behandlas med eftertanke. I affärsvärlden kan rätt information vid rätt tidpunkt innebära skillnaden mellan vinst och förlust, framgång och misslyckande. Informationssäkerhet bidrar till att säkra och skydda informationen mot oavsiktlig eller uppsåtlig ändring, utplånande och mot obehörigt avslöjande. Genom att skydda sin information kan man förhindra att företagshemligheter läcker ut och kommer i fel händer. Caveo (2003) skriver att i Februari 2000 tappade U.S. State Department bort en bärbar dator som innehöll flera tusen sidor hemligstämplad information. Datorn hade inte ens lösenordsskydd och informationen var inte krypterad. Denna och liknande händelser får en att reflektera om hur omfattande problematiken är i realiteten.

Under de senaste åren har den säkerheten på den tekniska informationssystemsnivån avsevärt förbättrats. Detta i samband med att organisationer blivit tvungna till mer avancerad teknik för att skydda sig, på grund av att med att metoderna för intrång har blivit mer avancerade. Ett område där säkerheten inte har förbättrats är skyddet mot attacker inifrån organisationerna själva (Samhällets informationssäkerhet Lägesbedömning, Krisberedskapsmyndigheten 2006). Det handlar om problem som bottnar i organisationens sätt att hantera information, detta innebär i praktiken att säkerheten inom en organisation inte är starkare än den svagaste länken.

Med dagens tillbehör kan vi lätt och enkelt arbeta var vi än befinner oss. Dagens mer mobila datorer hjälper oss att utnyttja och flytta vår information med väldigt enkla medel. Kan denna bekvämlighet göra att vi inte inser vilka säkerhetsrisker som kommer med användandet av mobila enheter? Enligt SCB är distansarbete mycket vanligt i de svenska storföretagen (fler än 500 anställda), upp till 90 % av storföretagen har personal som distansarbetar med hjälp av datorer. Bland företag med tio anställda eller fler är det 40 % av företagen som har personal som distansarbetar (Företagens användning av datorer och Internet, SCB, 2005).

En del av problematiken ligger i att vi använder Internet allt mer i vår dagliga arbete, vi är på det viset sammankopplade i ett enda stort nätverk. Enligt SCB har de 82% av de svenska företagen med fler än tio anställda tillgång till bredbandsanslutningar, och vart fjärde företag använder också mobiltelefonnätet för att exempelvis ge anställda som ute och reser tillgång till Internet (Företagens användning av datorer och Internet, SCB, 2005).

I Teliasoneras trendspaning 2006 (Teliasonera trendspaning, 2006) ser vi en trend i att mer än 25 procent av företagen i Sverige vill investera mer i elektronisk kommunikation och speciellt i bärbara datorer till sina anställda, snabbare bredband och e-post i mobilen. De har också funnit att allt fler använder mobila tjänster som e-post och Internet när de använder sina mobiltelefoner, och att allt mer människor kopplar upp sig till arbetsplatsen från distans. Detta öppnar upp en helt ny nivå för attacker mot företagen i form av stulen hårdvara, användning av hårdvaran utanför företagets till synes säkrade miljö, att obehöriga personer använder hårdvaran etcetera. Det kan handla om att en anställd tar hem sin dator över helgen, och någon i hans familj i god tro installerar ett program som sedan visar sig vara en säkerhetsrisk. Ett annat scenario är att en anställd sitter på ett trådlöst nätverk på exempelvis ett hotell, ett nätverk där kommunikationen inte skickas krypterad samtidigt som en fientligt inställd konkurrent avlyssnar kommunikationen. Har all denna förändring mot ett mer mobilt användande av informationsteknik skapat nya hot

eller bara intensifiering av tidigare funna hot? BITS är av intresse att undersöka just för att den har kommit i en ny reviderad version och användandet av mobila enheter och nya tekniker som trådlösa nätverk fortsätter öka. BITS bör således även kunna vara ett stöd vid användandet av mobila enheter inom organisationer.

1.2 Syfte

Syftet med denna uppsats är att utreda huruvida Krisberedskapsmyndighetens Basnivå för informationssäkerhet (BITS) klarar av att hantera informationssäkerhetsproblematik kopplat till användandet av mobila enheter.

1.3 Frågeställningar

Hur förhåller sig BITS i förhållande till användandet av mobila enheter?

Vad är den övergripande problematiken med informationssäkerhet och mobila enheter?

1.4 Målgrupp

Uppsatsen är främst utformad för läsare som redan har viss kunskap inom informationssäkerhetsområdet. Tänkta läsare är studenter inom datorrelaterade utbildningar och människor som arbetar med informationssäkerhet ute i organisationer. Framför allt personer som i sin yrkesroll har säkerhetsansvar och önskar få sig en aktuell bild av informationssäkerhetsproblematiken.

1.5 Avgränsningar

Krisberedskapsmyndigheten (KBM) delar upp informationssäkerhet i tre nivåer. Informationssystemnivå, organisationsnivå och samhällsnivå (Krisberedskapsmyndigheten Samhällets informationssäkerhet, 2006). Vi har valt att enbart fokusera på nivåerna gällandes informationssystem och organisation. Informationssystemnivån innebär informationssystemen i fråga och innefattar skadlig kod, mjuk- och hårdvara etcetera. Vi kommer dock inte att fokusera på hårdvara inom informationssystemsnivån i speciellt stor utsträckning. Organisationsnivå innefattar organisationen och dess medlemmars påverkan på informationssäkerheten. Vidare avgränsar vi informationssäkerhet till endast de definitioner som innebär att informationsteknologi på något sätt är inblandad, Lenanders (1998) definition där informationssäkerhet är ett samlingsbegrepp för hur all information hanteras använder vi inte. Undersökningen behandlar endast de delar av BITS som vi fann relevanta för våra frågeställningar.

1.6 Disposition

Vi valde att bygga upp vår uppsats med en lineär struktur. För att underlätta för läsaren och ge en överblick av vår uppsats går vi här igenom hur vi strukturerade upp kapitelindelningen.

Inledning (kapitel 1)
Vi genomför en förklaring kring bakgrunden och problemområdet kring vårt valda ämne. Här finner man även vårt syfte med uppsatsen, allt för att ge en klarare bild om varför vi valde att skriva denna uppsats.

Metod (kapitel 2)
Under detta kapitel går vi igenom vårt val av metod och hur vi gick tillväga för att samla in informationen som ligger till grund för vår undersökning.

Teorin (kapitel 3-4)
Här går vi igenom bakgrunden till informationssäkerhet och mobila enheter för att ge en klarare bild av hur problemområdet ser ut. Vi förklarar även mera ingående kring basnivån för informationssäkerhet från Krisberedskapsmyndigheten (BITS). För att sedan sätta det i perspektiv med vår undersökning (kapitel 4). I undersökningen jämför vi BITS med vad som framkom under våra expertintervjuer, detta för att identifiera eventuella brister, förbättringar eller bekräftelse på hur BITS hanterar informationssäkerhetsproblem kopplade till användandet av mobila enheter.

Slutsats (kapitel 5)
Med hjälp av analysen av expertintervjuerna vi genomförde i kapitel fyra presenterar vi här en slutsats som besvarar våra frågeställningar och vårt syfte. Vi föreslår här även förslag på vidare forskning inom området.

Bilagor
Begreppsteorin skall vara till hjälp för eventuella tekniska termer och förkortningar som finns i uppsatsen och som kan vara svåra att förstå. Här finner man även transkriberingarna från våra expertintervjuer samt vår referenslista.

2 Metod

Vi valde att studera informationssäkerhetsproblematik kopplat till användandet av mobila enheter genom att först undersöka ämnet utifrån relevanta och i vår mening tillförlitliga publikationer. Med bas i denna information och i litteratur för kvalitativa intervjuer tog vi fram ett frågeunderlag till expertintervjuer med inom branschen yrkesverksamma personer. Tre expertintervjuer med mycket erfarna och inom informationssäkerhetsbranschen aktiva yrkesmän på tre stora internationella företag genomfördes. Efter detta analyserades det empiriska materialet med utgångspunkt i våra frågeställningar och de för frågeställningarna relevanta delarna av BITS.

2.1 Metodval

Att välja rätt metod för sin forskning är kritiskt för analyserandet av undersökningsmaterialet, då den metodologiska utgångspunkten påverkar vad forskaren uppfattar som ett problem, i vilket sammanhang problemet undersöks och hur undersökningsfrågorna utformas. Svaren till det undersökta kommer att inskränkas av dessa ramar men kommer också att förtydliga eller dölja omständigheterna som forskaren undersöker (Holme *et al.*, 1997).

De traditionella metoderna är antingen kvantitativa eller kvalitativa i sin utformning. Båda dessa metoder skall kartlägga och analysera olika fenomen hos det som ska studeras. Den största skillnaden mellan dessa två metoder är att den kvantitativa tolkar medan den kvalitativa metoden beskriver (Bryman, 1997)(Holme *et al.*, 1997). En blandning av dessa två metoder är också möjlig.

Kvantitativa metoder utnyttjar strukturerade frågor som verktyg för skapandet av en empiri och utrycker oftast informationen i statistik och siffror (Halvorsen, 1992). Man skickar ofta ut större mängder med frågeformulär där respondenterna får svara på olika svarsalternativ. Med hjälp av dessa resultat hittar man ett medelvärde som ger en generell bild av problemet man vill undersöka. Att göra några djupare tolkningar från dessa svar är svårt eftersom man gärna fokuserar på icke-kvantifierbara egenskaper, Bryman (2002). Vidare anser Bryman att för att få en djupare insikt och förståelse för den verklighet som skall studeras skall forskaren använda sig av en kvalitativ studie. På grund av det har vi valt att göra vår undersökning om den aktuella informationssäkerhetssituationen kvalitativt orienterad.

I våra intervjuer med experterna inom informationssäkerhet anser vi att den kvalitativa metoden ger oss ett större djup inom det aktuella problemområdet. Kvalitativ analys är en induktiv process där motiv utvecklas allt eftersom det undersökta analyseras. På så sätt återkommer forskaren hela tiden till sin data med nya frågor och förändrade perspektiv under analysprocessen (Freeman *et al.*, 2003). Vi kommer därför att utnyttja ett induktivt arbetssätt, detta kännetecknas av att vi kommer att studera objektet och därefter, utifrån insamlad information, försöka formulera en teori (Freeman *et al.*, 2003).

2.2 Datainsamling & Val av litteratur

2.2.1 Val av litteratur

Det faktum att nulägessituationen när det gäller informationssäkerhet på informationssystemnivån förändras i rasande takt gjorde det svårt för oss att hitta uppdaterad tryckt litteratur. Mycket publiceras i elektroniskt format i form av rapporter från myndigheter och säkerhetsföretag.

Detta faktum gjorde det svårt att hitta tillförlitliga och uppdaterade böcker inom ämnet och för att vi skulle få möjlighet att studera problematik på informationssystemsnivån kopplat till mobila enheter valde vi i stor utsträckning att förlita oss på att samla in empiriskt material, genom tre expertintervjuer med inom informationssäkerhetsbranschen verksamma och kunniga yrkesmän. Intervjuobjekten blev Magnus Lindkvist som är nationell säkerhetschef på Microsoft Sverige AB ,Per Hellquist, säkerhetsspecialist på Symantec samt Johan Jarl säkerhetsspecialist på F-Secure.

När det gäller valet av litteratur för att studera problematiken på den organisatoriska nivån använder vi oss av Basnivå för informationssäkerhet (BITS) som är framtagen av Krisberedskapsmyndigheten (KBM) och baseras på säkerhetsstandarden SS-ISO/IEC 17799.

Eftersom vi ville ha tillförlitliga och aktuella källor när det gäller litteratur fick vi rikta in oss på rapporter och andra publikationer publicerade av stora och välrenommerade företag och organisationer, rapporter som vi ofta fann via Internet. Det är detta som Backman (1998) kallar för formella skriftliga källor, vilket han anser ger bäst grund för en vetenskaplig ansats. Det finns risker med tillförlitligheten i dokument hämtade via Internet och för att styrka reliabiliteten i källorna anser vi att det är troligare att publikationer med välkända upphovsmän har genomgått en högre form av granskning.

För att få fram material inom ämnet använde vi således de två metoder som Backman (1998) kallar konsultation och datorbaserad sökning. Konsultation i form av de tre intervjuerna och datorbaserad sökning i referensdatabaser och andra elektroniska kanaler. Vi valde konsultation på grund av att vi ville få fram den aktuella bilden av informationssäkerhetssituationen och datorbaserad sökning för att få underlag till intervjuerna samt utöka vår teoretiska bas.

2.2.2 Primär- och sekundärdata

All information som samlas in kan kategoriseras som antingen primärdata eller sekundärdata (Holme et. al, 1997). De menar att information som samlas in av forskarna direkt klassificeras som primärdata. Information som tidigare är insamlad och publicerad är sekundärdata. Vår teoretiska bas är således uppbyggt av primärdata i form av våra intervjuer. Primärdata hämtades således från vår empiri.

Vi använde sekundärdata för att få fram ett underlag för skapandet av primärdata. Exempelvis statistik framtagen av olika företag. Att använda sekundärdata som en grund för att få fram primärdata nämns av Backman (1998) som ett bra tillvägagångssätt för att genomföra datainsamling. Sekundärdata användes även till viss del till att styrka våra slutsatser.

2.3 Expertintervjuer

Intervjuerna bedrevs efter ett kvalitativt arbetssätt, en semistrukturerad intervjuform (Bryman , 2002). Bryman menar att semistrukturerade intervjuer innebär att intervjuaren har en uppsättning frågor som kan liknas vid ett frågeschema. Frågorna är också mer allmänt formulerade och ger en större möjlighet till tolkning hos intervjuobjektet, vilket kan resultera i mer målande och djupgående svar än vid en strukturerad intervju. Vidare menar Bryman att det också ger intervjuaren möjlighet att under intervjuns gång ställa ytterligare frågor vilket vi anser kan resultera i en djupare förståelse för det ämne som intervjun berör. Detta angreppssätt ville vi använda för att verkligen kunna få insikt i ämnet, framförallt i intervjuerna med de tre yrkesmännen. Vid en kvalitativ intervjuform utövar forskare relativt lite styrning och försöker få intervjuobjekten att forma samtalet, forskaren ska dock se till att få svar på de frågor han vill ha svar på, detta får intervjun att likna ett vanligt samtal och det är en av fördelarna med en kvalitativ intervjuform (Holme *et. al*, 1997). Intervjuerna genomfördes med hjälp av IP-telefoni och programvaran Skype, vi spelade även in intervjuerna för att kunna transkribera dem. Samtalslängden per samtal var i snitt en och en halv timme.

2.3.1 Transkribering och kodning

Under analysen av intervjuerna använde vi öppen kodning för att få möjlighet att kategorisera upp vår empiri, för att i slutändan få en djupare förståelse. Öppen kodning är en teknik för att bryta ner, studera, jämföra, konceptualisera och kategorisera data (Bryman, 2002). Vi transkriberade intervjuerna i talspråk vilket stöds av Bryman (2002) som menar att det är viktigt att säkerställa att transkriberingen är korrekt, vi lyssnade även igenom dem för att undersöka om vi hade missat något. Efter det fick informanterna läsa igenom transkriberingarna för att säkerställa att vi hade uppfattat allt korrekt. När vi påbörjade vår analys och kodning försökte vi först att hitta begrepp som återkom på flera ställen i intervjuerna. Vi fick fram huvudbegrepp som utbildning, informationssäkerhetspolicy, lager-på-lagersäkerhet etcetera. Efter det började vi kategorisera stycken i intervjuerna med olika kategorier, kategorierna var hämtade från de delar av BITS som vi hade funnit centrala genom vår genomgång av just BITS. Ett textstycke kunde höra till flera olika kategorier, dessa kategorier ställdes sedan mot varandra för att vi skulle få möjlighet att se fler samband.

2.3.2 Intervjupersoner

Vid valet av intervjupersoner för att samla in våra primärdata ville vi intervjua personer på stora internationella företag, detta på grund av att informationssäkerhet är ett internationellt problem utan synliga gränser. Vi valde Microsoft för att de är världens ledande tillverkare av mjukvara och deras operativsystem och serverlösningar har stora marknadsandelar, väldigt många företag använder deras produkter. En annan anledning som gör Microsofts åsikter extra intressanta är att de har fått utstå mycket kritik för att deras mjukvara haft stora brister i säkerheten. Symantec och F-Secure valdes som motpol till Microsoft, två renodlade säkerhetsföretag, företag som också producerar och tillhandahåller mjukvara som används i ett stort antal informationssystem runt om i världen.

2.3.1.1 Intervju Magnus Lindkvist, Microsoft Sverige AB

Magnus Lindkvist arbetar som Cheif Security Advisor på Microsoft AB, vilket i praktiken innebär att han är nationell säkerhetsexpert, en strategisk roll mot storkunds och privatpersons marknaden. Magnus har arbetat på Microsoft AB sedan mitten av 90-talet, bland annat tjänstgjort som Security Program Manager på Microsofts globala incidentcenter Microsoft Security Response Center i USA. Han började sin karriär på Microsoft med att arbeta med säkerhet gällandes dess webbserver Internet Information Service.

2.3.1.2 Per Hellqvist, Symantec Nordic AB

Per Hellqvist är säkerhetsspecialist på Symantec Nordic AB och har tidigare arbetat på bland annat F-Secure. Han är specialiserad på mobil säkerhet, skadlig kod, virus och trojaner. Han talar frekvent på konferenser, seminarier och har blivit en känd profil inom IT-säkerhetsbranschen. 2004 tilldelades han SigSecuritys säkerhetsstipendium och 2005 fick han mottaga Näringslivets Säkerhetsdelegations säkerhetsstipendium. Symantec är en av världens ledande leverantörer av tekniska säkerhetslösningar och tjänster till privatpersoner och företag och bedriver verksamhet i 40 länder. Han drev under lång tid e-postlistan Svenska Viruslistan (SVL). SVL var en e-postlista dit större organisationer och företag i Sverige rapporterade sina aktuella virusproblem, information som sedan Per Hellqvist sammanställde i veckorapporter. Han driver även en blogg om säkerhet med namnet Svenska Viruslistans Blogg, där han publicerar aktuella informationssäkerhetsrelaterade nyheter.

2.3.1.2 Johan Jarl, F-Secure

Johan Jarl har arbetat med informationssäkerhet sedan 1999 och började sin karriär på säkerhetsföretaget ProtectData och arbetar sedan 2002 som säkerhetsspecialist på säkerhetsföretaget F-Secure. F-Secure är ett globalt säkerhetsföretag grundat 1989, verksamheten är inriktad på att stödja privatpersoner och företag mot säkerhetshot relaterat till Internet och mobila lösningar.

2.4 Reliabilitet och validitet

Reliabilitet definieras av Patel & Davidson (1994) som hur väl mätinstrumentet motstår inverkan av slumpen. Det vill säga att inom testningar och mätningar anger reliabiliteten metodens tillförlitlighet i mätningen. Till exempel så skall resultatet vara detsamma vid upprepade mätningar (*test-retest-reliabilitet*), oberoende av vem som utför testet (*interbedömarreliabilitet*).

Eidersheim-Paul & Eriksson (1997) menar att validitet är ett begrepp som definieras som mätinstrumentets förmåga att mäta det man avser att mäta. Validitet kan generellt sägas vara ett mått på hur väl man mäter det man vill mäta, validiteten kan uttryckas som korrelationen mellan den teoretiska definitionen och den operationella definitionen.

Det råder olika meningar i forskningsvärlden om hur viktig reliabilitet och validitet är för kvalitativa studier. Reliabilitet och validitet är viktiga kriterier för en kvantitativt inriktad forskning för att få en bild av kvaliteten i en undersökning. Många kvalitativt inriktade forskare har dock haft en diskussion om hur pass relevanta dessa begrepp är för kvalitativa undersökningar

(Bryman, 2002). Svenning (1996) anser att god validitet är viktig i båda fallen eftersom de personer som intervjuas måste vara relevanta för undersökningen. Resultaten från dessa intervjuer måste vara användbara, reliabla, tillförlitliga och valida (Svenning, 1996). Trost (1997) anser att de traditionella definitionerna på reliabilitet och validitet härstammar från kvantitativ metodologi, därav menar han att de inte går att mäta på ett bra sätt vid kvalitativa studier.

Vi kommer att tillämpa alternativa kriterier för bedömningen av våra kvalitativa undersökningar. Guba & Lincon (1994) anser att der är nödvändigt att specificera termer och metoder för att analysera och bedöma kvaliteten i kvalitativ forskning som utgör ett alternativ till det som begreppet reliabilitet och validitet står för. De föreslår istället två andra grundläggande kriterier för bedömning av en kvalitativ undersökning, nämligen trovärdighet och äkthet. Trovärdighet består av fyra delkategorier.

- Tillförlitlighet

  Att skapa en tillförlitlighet i resultaten och intervjuerna inbegriper både att man säkerställt att forskningen och intervjuerna utförts i enlighet med de regler som finns och att man rapporterar resultaten till de personer som är en del av den sociala verklighet som studerats för att dessa ska bekräfta att forskningen uppfattat denna verklighet på ett riktigt sätt (responsvalidering).

- Överförbarhet

  Kvalitativa forskningar tenderar att fokusera på det kontextuellt unika och på meningen hos, eller betydelsen av den aspekt i den sociala verkligheten som studerats. Guba och Lincon menar på att en uttömmande redogörelse kan förse andra personer med något som författarna kallar en databas. Med hjälp av denna kan de sedan bedöma hur pass överfarbara resultaten är till en annan miljö.

- Pålitlighet

  Kan ses som en motsvarighet till reliabilitet inom kvantitativ forskning. Pålitlighet innebär att forskarna har ett granskande synsätt och under processens gång väl dokumenterar alla faser av forskningsprocessen, exempelvis producerar dokument med fältanteckningar, val av undersökningspersoner, intervjuutskrifter etc.

- Möjlighet till att styrka och konfirmera

  Forskaren utgår från att det inte går att ha fullständig objektivitet i samhällsvetenskaplig forskning, utan forskaren ska försöka säkerställa att denne agerat i god tro. Forskaren ska inte medvetet låtit sina personliga värderingar och teoretiska hemvist påverka undersökningen eller analysen av resultatet.

Kriteriet äkthet berör enligt Guba & Lincon (1994) några generella frågor om forskningspolitiska konsekvenser. Som exempelvis om forskningen ger en rättvis bild av olika uppfattningar inom det man undersöker hjälper forskningen till med att öka förståelsen för den sociala situationen hos de man undersöker.

Vi har valt att applicera grundkriterierna från Guba & Lincon (1994) på vår undersökning. Tillförlitlighet nås genom att intervjuobjekten i god tid har vetat om intervjun samt att de efter analys av intervjuerna har fått läsa igenom dem och komma med kommentarer och åsikter. Överförbarhet får vi genom att väl dokumentera intervjuprocessen, intervjuerna spelades in på band för att sedan transkriberas. Pålitlighet får undersökningen genom att vi i vårt arbete dokumenterat och motiverat vårt val av personer. Det faktum att vi har ett induktiv synsätt leder till en möjlighet att styrka och konfirmera vårt arbete, vi har arbetat med utgångspunkt att vi vill

undersöka den faktiska verkligheten och inte verkligheten som vi uppfattade den när processen startade. Kriteriet äkthet har enligt Bryman (2002) inte haft någon större betydelse för forskningen och vi kan inte se att vi nått äkthet på annat sätt än genom att vi försökt ge en rättvis bild av flera olika sidor, vi valde tre företag med olika uppfattningar, två renodlade säkerhetsföretag och ett mjukvaruföretag.

Per Hellqvist, Magnus Lindkvist och Johan Jarl kan ses som tre av Sveriges mest kunniga personer inom ämnet, vår uppfattning är att de är tre mycket goda val för vår undersökning.

2.5 Källkritik

Källkritikens syfte är att kunna se till att källor är korrekta i sina antaganden, det är en av orsakerna till att när vi har förlitat oss till litteratur har vi endast tagit litteratur från välrenommerade företag och organisationer, mycket på grund av att diverse publikationer hämtats i elektronisk form. När det gäller valet av litteratur för att studera problematiken på den organisatoriska nivån använder vi riktlinjerna för Basnivå för informationssäkerhet (BITS) som är framtagen av Krisberedskapsmyndigheten (KBM). BITS har hittills lett till att de flesta kommuner och alla länsstyrelser har styrande dokument för informationssäkerhet, baserade på rekommendationerna i BITS (Krisberedskapsmyndigheten, 2006) och detta bör således ses som att det är väl beprövade riktlinjer med bas i organisationers vardag.

Intervjupersonerna på Microsoft AB, Symantec Nordic AB och F-Secure representerar företagsintressen, vilket kan ses som ett problem. Men eftersom de representerar tre stora och betydelsefulla marknadsaktörer bör deras åsikter ses som en tungt bidrag i debatten om informationssäkerhet. Väldigt många företag och människor påverkas varje dag av företagens produkter och tjänster, på ett eller annat sätt. Det faktum att företagen är helt oberoende sinsemellan, de har inget internt beroende av varandra, befäster att deras separata åsikter är ett viktigt bidrag. Vi får på våra frågeställningar tre skilda infallsvinklar, infallsvinklar som har sin grund i hur tre av världens inom ämnet mycket betydelsefulla företag uppfattar den aktuella situationen.

Att intervjuerna genomfördes via telefon kan ses som en brist i vår undersökning. Vi valde telefonintervju på grund av avståndet till Stockholm, samt att personerna i fråga är väldigt upptagna och i långa perioder är ute och reser. Bryman (2002) riktar kritik mot telefonintervjuer och menar att problemen är bland annat att det finns risk för att urvalsproceduren urlakas. Vidare nämner han också problemet med att man inte kan visuellt observera intervjuobjektet och analysera dennes ansiktsutryck etc. Det finns även fördelar med telefonintervjuer, Bryman (2002) nämner tidsåtgången och den låga kostnaden som exempel på fördelar, en annan fördel han poängterar är den att vid en telefonintervju kan inte respondenternas svar påverkas av hans uppfattning om vilka personliga egenskaper intervjuaren verkar besitta, klass, ålder, etnisk bakgrund etcetera.

3 Informationssäkerhet och mobila enheter

3.1 Bakgrund till informationssäkerhet och mobila enheter

För att vi skulle få mer insyn inom ämnet innan intervjuerna genomfördes ville vi få reda på mer om säkerhetsproblematik kopplat till användandet av mobila enheter. Skulle en term vara främmande finns beskrivningar av begrepp och förkortningar i Bilaga 1, Begrepp.

Med mobilitet kommer också trådlösa nätverk in i bilden och användandet av det fortsätter att öka, företag använder sig mer och mer av trådlösa nätverkslösningar för att få ner kostnader och för att ge anställda frihet att arbeta var som helst på arbetsplatsen via sina bärbara datorer eller PDAs (Personal Digital Assistant). Universitet och skolor använder sig ofta av trådlösa nätverk för att ge studenterna möjlighet att snabbt och enkelt kolla upp den information de behöver. Men på senare tid har de trådlösa nätverken även börjat dyka upp på platser som caféer, busstationer, restauranger, till och med allmänna torg erbjuder trådlösa nät. Trådlösa nätverk är väldigt enkla och praktiska att använda, dock har de tyvärr en hel del negativa sidor (Boeckeler, 2004).

Organisationer har de senaste åren spenderat stora resurser på att säkra sinn interna infrastruktur från externa attacker. Idén kring detta är enkel, genom att begränsa antalet externa anslutningarna kan företagen relativt enkelt kontrollera trafiken. Men med trådlösa nät ökar riskerna för att det öppnas en bakdörr in till företagets nätverket, vilket i sin tur skapar fler möjligheter till attacker utifrån. Utan att den som försöker ta sig in har fysisk access till någon av organisationens nätverksanslutningar (Arbaugh *et. al.*, 2001). Arbaugh *et. al.* (2001) anser ironiskt nog att i några fall är en brandvägg i ett trådlöst nätverk mer sårbar för attacker utifrån eftersom man ofta anser att man är immun mot attacker utifrån.

Säkerhetsinställningar som finns i produkter för trådlösa nätverk används inte i någon stor utsträckning enligt Samhällets informationssäkerhet, Lägesbedömning, (Krisberedskapsmyndigheten, 2006). Samma rapport belyser även att det finns ett stort behov av att öka säkerhetsmedvetandet i samband med användningen av trådlösa nätverk. Hurley et al. (2004) menar att trådlösa nätverk har blivit väldigt vanligt de senaste åren och behovet av att hålla dem säkra bara ökar. De nämner tekniker som WarDriving som ett hot mot trådlösa nätverk, det innebär att en person letar efter trådlösa nätverk inom ett område för att sedan möjligtvis försöka infiltrera dem, väl inne kan personen stjäla information, använda Internetanslutningen för eget bruk etcetera. Danielson (2002) menar att med användande av handhållna enheter kommer ökat användande av trådlösa nätverk, vilket enligt honom ökar säkerhetsriskerna. Detta på grund av att tekniken som trådlösa nätverk bygger på innebär att information bokstavligt talat skjuts ut ur företagen när den färdas genom luften. Informationen måste krypteras och man måste förhindra intrång i företagets nätverk, problematiken skiljer sig från den vid traditionella nätverkslösningar menar han.

Det finns två fundamentala komponenter som man måste tänka på när man skyddar sitt trådlösa nätverk. Det första är att se till att ovälkomna enheter inte kan kopplas upp emot nätverket. Det finns flera olika sätt att förhindra detta, ett sätt är att registrera de datorer som får utnyttja routern eller att helt enkelt stänga av den automatiska SSID sändningarna. Det andra är att se till att ingen

avlyssnar din trafik och försöker stjäla känslig data från ditt nätverk. Till exempel är WEP (Wired Equivalent Privacy) ett protokoll som används för att förebygga detta (Boeckeler, 2004).

De flesta företagen placerar mobilitet bland sina högst prioriterade initiativ för de kommande tre åren (Gold, 2006). Däremot har få företag insett att dessa initiativ för förbättrad mobilitet, som skall ge ökad produktivitet, sätter företaget i en mycket större säkerhetsriskzon än tidigare. Användandet av så kallade smarta telefoner (BlackkBerry, Treo, Nokia Communicator etcetera) har ökat dramatiskt inom de flesta organisationer enligt Gold (2006). Detta innebär att företagen måste erbjuda fler uppkopplingsmöjligheter för dessa användare och det tillkommer nya krav på säkerhet då det ofta gäller externa eller trådlösa anslutningar. Enligt Gold (2006) erbjuder de flesta av dessa enheter inte adekvat säkerhet vilket ställer till problem för företagen. Även allt fler av dessa enheter stödjer flyttbara minneskort vilket ökar de potentiella säkerhetsriskerna eftersom det är oerhört svårt, nästintill omöjligt, för organisationen att hålla reda på vart informationen på dessa och vart själva enheterna tar vägen.

Enligt Gold (2006) är en orsak att informationssäkerhet kopplat till mobila enheter såsom smarta telefoner är komplext är det faktum att användarna ofta själva är med och införskaffar enheterna, och använder dessa både privat och i tjänsten. Just att enheterna kan lagra mycket information gör dem attraktiva för användare och företag, men medför även större risker för företagen menar Gold (2006). Det är inte heller ovanligt att användare laddar ner filer från arbetet till sina mobila enheter antigen för att säkerhetskopiera eller för att senare fortsätta arbeta med informationen på en annan dator. Men ofta sker detta utan att företagen vet om det och utan företagets kontroll eller spårning (Gold, 2006). Att man just förlorar stora delar av kontrollen på vart informationen finns är ett stort problem med mobila enheter enligt författaren.

Intrång i företagets nätverk har varit ett växande problem de senaste åren. Vad som är uppenbart är att säkerhet är ett ökande problem som tidigare för det mesta berört borttappade säkerhetskopior, intrång i företagets servrar eller helt enkelt insiderbrott. Det mesta sker i en relativt kontrollerad och instängd miljö. Men med flytten till mobilitet, med väldigt många fler enheter som har möjligheten att vara utanför företagets kontrollerade miljö, kommer dataintrångsmöjligheterna att öka, varav flera inte ens är identifierade eller kommer att identifieras på att bra tag framöver. Så företagen måste formulera en mobil strategi innan problemen blir överväldigande (Gold, 2006). Majoriteten av säljare i företagen använder sig av mobila enheter. Dessa enheter innehåller ofta kundregister och annan finansiell information som kan vara känslig. Det är inte ovanligt för säljare att ha ett svinn på 25 % av enheter per år (Gold, 2006). Vidare menar Gold att mobila intrång eller förluster även är svårare att identifiera och det händer att användaren inte märker att man är av med någonting förrän dagar eller veckor senare.

Mobilitet i sig själv är ett hot mot informationssäkerheten enligt Price (2003), just för att mobiliteten gör det svårt att ha kontroll över enheterna och att de ofta använder sig av trådlösa nätverk. För att överbygga bristerna i många av de trådlösa teknikerna kan man enligt Price använda sig av VPN-uppkopplingar för att kommunicera mellan olika nätverk, kryptera informationen när den skickas. Ett annat hot Price tar upp är skadlig kod som kan infektera en mobil enhet, man måste skydda sig mot detta för att förhindra skada inom företagets nätverk. Price nämner att 250 000 mobila enheter blev borttappade eller kvarglömda på amerikanska flygplatser under 2001, problemen ligger enligt Price till stor del i risken att förlora information. Information som kan hamna i fel händer, och för att förhindra obehörig åtkomst till informationen måste man kryptera känslig information.

Säkerhetsföretaget PointSec rapporterar om problematiken kopplat till information lagrat på mobila enheter och om dessa enheter skulle hamna i fel händer, man måste ta i beräkning vilken

skada informationen på dessa enheter kan orsaka om den sprids ut över världen utanför företagets kontroll (PointSec, 2004). De påpekar att känslig information på alla enheter som kan tas ut från företages nätverk ska krypteras. Wayne Jansen *et. al* (2004) menar att mobila enheter har stora brister när det kommer till säkerhet, de menar att kryptering av informationen är en central fråga som väldigt många helt enkelt missar. Vidare är Wayne Jansen *et. al* (2004) av åsikten att andra metoder såsom inloggningsskydd, förbättrad autentisering av användarna också ska has i åtanke. Om en enhet tas ut ur företagets nätverk och efter det kopplar upp sig mot Internet kan den utsättas för olika säkerhetshot. I Protecting Against Complex Internet Threats (Websense, 2005) nämns att när en enhet tas ut från företagets nätverk förlorar den det perimeterskydd som företaget har byggt upp för att försäkra sig om hög informationssäkerhet. Enligt dem finns det också en problematik med att anställda mycket ofta måste använda Internet för att utföra sitt dagliga arbete. När de gör detta kan de utsätta arbetsgivaren för allvarliga risker, det finns risker såsom virus och trojaner som sprids via e-post, skadlig kod kan finnas på webbplatser de besöker etcetera.

Bergman & Hagström (2005) lägger fram att antalet stölder av bärbara datorer ökar varje år, likadant med försäljningen av dessa. De menar att företag har en mycket svår utmaning i att på ett effektivt sätt skydda känsligt innehåll på dessa enheter. Kryptering är något som författarna framhåller som en lösning för en del av problemen kopplade till mobila enheter. En annan viktig punkt enligt Bergman & Hagström (2005) är utbildning av användarna i hur de ska använda sina bärbara enheter tillsammans med informationssäkerhetstänk. Att bristen på utbildning av användare är ett problem belyses även i Samhällets informationssäkerhet, Lägesbedömning (Krisberedskapsmyndigheten, 2006). De menar att organisationer förväntar sig att användarna ska klara av att hantera systemen även om de inte har fått någon utbildning i det. Det är de oavsiktliga hoten som ökar, detta på grund av bristande användarutbildning enligt Krisberedskapsmyndigheten.

I rapporten Secutiry for Mobile Devices (Trend Micro, 2005) belyses det att mobila enheter som mobiltelefoner och PDAs blir allt mer avancerade, de kan lagra mer information, de är ansluta till Internet. De mobila enheterna är idag små avancerade datorer. Med mobilitet kommer ju också det faktum att dessa enheter flyttas ut ur företaget och ansluts till andra nätverk än företagets egna, dessa punkter har medfört nya hot mot informationssäkerheten enligt Trend Micro. Bland annat för att dessa enheter och dess mjukvara ofta är framtagna utan att tillverkarna har beaktat säkerhetsfrågor. Rapporten nämner hot som att enheten kan bli stulen, borttappad eller infekterad av skadlig kod som exempelvis virus och maskar. Hoten resulterar i reducerad produktivitet då det ofta är tidskrävande och svårt att återställa informationen. Dock menar de att kostnaden kan bli mycket större om den förlorade enheten skulle innehålla känslig information, information som skulle kunna skada företaget. Om en enhet skulle bli infekterad av skadlig kod finns det ett stort hot i detta, den smittade enheten riskerar att infektera övriga enheter i företagets nätverk. Detta hot ställs på sin högkant när företag använder mobila enheter som flyttas ut och in från företagets domän. Skadlig kod sprids enligt Trend Micro till enheterna via tillgång till Internet, användarna använder ofta mobila enheter till annat än sina arbetsuppgifter. För att skydda mobila enheter måste man enligt rapporten kryptera informationen som finns lagrad på dem, om trådlösa nätverk används måste även trafiken i dessa krypteras. Man måste även se till att det finns någon form av autentiseringsfunktionalitet så att inte vem som helst kan använda enheterna.

När det gäller mobiltelefoner och PDAs ska det finnas en återställningsfunktion som kan initieras från distans, återställningsfunktionen använder man om en enhet med känslig information skulle förloras. Återställningsfunktionen raderar all information på enheten och förhindrar att känslig information kommer i fel händer. För att skydda sig mot hoten som uppkommer vid

användandet av mobila enheter måste ett företag klassificera data och hålla kontroll på vem som har den och på vilka enheter den finns lagrad. Man måste också etablera en säkerhetspolicy som hanterar användandet av mobila enheter där det specificeras användaransvar, hur enheterna ska användas, vilken programvara som får installeras etcetera. En annan punkt som rapporten poängterar är att företag måste utbilda sina anställda i hur de använder mobila enheter och vilka risker som finns i detta, vad som kan hända om de inte följer säkerhetspolicyn. Företagen måste också implementera en barriär av skydd på varje enskild enhet, antivirusprogram, brandvägg, autentisering, kryptering och mjukvaran måste vara uppdaterad (Trend Micro, 2005).

Med mobilitet blir ofta distansarbete en naturlig effekt, företag vill låta sina anställda arbeta hemifrån eller när de är på resande fot (Teliasonera trendspaning, 2006). Rosenberry (2003) menar att man måste se till att skydda företaget från hot som kan uppstå vid distansarbete, även om man använder en VPN-uppkoppling för att ansluta sig till företagets nätverket utifrån. Normalt sett har man ett starkt perimeterskydd i företagets nätverk som skyddar mot attacker utifrån, man kan ha strikt kontroll på de anställdas datorer menar han. Men det går inte att ha denna kontroll i lika stor utsträckning när enheter ansluter utifrån. Hoten ligger enligt Rosenberry i att enheterna utanför företaget kan vara oskyddade mot de faror som finns i användandet av Internet, exempelvis skadlig kod. För att skydda enheter utanför företaget mot dessa hot ska man enligt Rosenberry se till att ingen obehörig får fysisk access till enheten, att exempelvis ingen familjemedlem använder enheten, eller att man inte utsätter den för att bli stulen, användaren måste vara medveten om risken att den blir stulen och vad det kan resultera i. Enheten ska även vara lösenordsskyddad, ha uppdaterat antivirusprogram och brandvägg. Han poängterar också vikten av att all mjukvara såsom operativsystem ska ha de senaste uppdateringarna installerade. För att åstadkomma detta måste man enligt Rosenberry skapa en säkerhetspolicy som reglerar hur användare ansluter till företagets nätverk utifrån, man måste enligt också se till att utbilda användarna om säkerhetspolicyn och informationssäkerhetsfrågor (Rosenberry, 2003). Även vikten av lösenordsskydd på enheter poängteras av Boeckeler (2004), han menar att man måste se till att användarna använder så kallade starka lösenord som är svåra att knäcka

Betydelsen av en säkerhetspolicy belyses även av Hietala (2004) som menar att en säkerhetspolicy är ett av medlen för högre informationssäkerhet. Just vid användandet av externa uppkopplingar mot företagets nätverk bör man ha specificerat i en policy vad som ska gälla för enheten som ansluter. Vilket typ av skydd den ska ha när det gäller antivirusprogram, brandvägg etcetera. Han belyser även att det är otroligt viktigt att ha brandväggar på varje enhet, speciellt när man använder mobila enheter, alla enheter inom företaget ska även ha uppdaterad mjukvara och antivirusprogram. Enligt Hietala (2004) bör man således använda sig av en lager-på-lagersäkerhet där man skyddar varje enskild enhet i sig själv, lik väl som man implementerar skydd som ska hantera många enheter som exempelvis företages brandvägg. Man förlitar sig således inte på att enbart ha ett starkt perimeterskydd utan man har flera lager av säkerhet som ska förhindra bland annat att utbrott av skadlig kod drabbar stora delar av nätverket. När det kommer till användandet av mobila enheter som har känslig information lagrad bör man enligt Hietala (2004) även ha tillförlitlig autentisering av användarna och kryptera informationen, för att förhindra att företagshemligheter läcker ut om enheten skulle tappas bort eller bli stulen.

Just lager-på-lagersäkerhet är något som Straub (2003) menar är centralt för en lyckosam informationssäkerhetsstrategi. Han menar att det går ut på att använda flertalet försvarsanordningar i flera olika lager i ett nätverks infrastruktur, för att skydda intern information, nätverket, informationssystem och användare. Fallerar ett säkerhetsskydd finns det fler lager av skydd, med uppgift att fortsätta skydda tillgångarna. Ett exempel är att ett företag kan ha ett centralt antivirusprogram som undersöker inkommande e-post, samtidigt som varje enhet i sin tur även har ett antivirusprogram. Om en mobil enhet blir infekterad utanför företagets

nätverk för att sedan tas in igen, ser lager-på-lagersäkerhet helt enkelt till att spridningen av hotet minimeras.

Att företag är oroliga över säkerhetsrelaterade frågor när det kommer till mobila enheter som tas in i företagets nätverk igen stöds av en rapport av säkerhetsföretaget Websense. De nämner att 71 % av de europeiska IT-cheferna är oroliga över säkerhetsrisker kopplat till användandet av mobila enheter när de återansluts till företagets nätverk. Men endast 21 % av företagen har policys eller produkter för att försäkra att dessa enheter är skyddade utanför företagets miljö ur ett informationssäkerhetsperspektiv (Websense, 2005). I Samhällets informationssäkerhet, Lägesbedömning (Krisberedskapsmyndigheten, 2006) fann de att skadlig kod numera sprids i större utsträckning av användare själva när de besöker förfalskade webbsidor eller laddar ner program som innehåller trojaner och dylikt. Detta är ett problem enligt dem då det är svårare att skydda sig mot denna typ av hot ur ett tekniskt perspektiv, exempelvis med hjälp utav brandväggar. Krisberedskapsmyndigheten belyser ytterligare vikten av utbildning på grund av detta faktum, för att få ett större säkerhetsmedvetande hos användarna.

Att företag står för en utmaning när det gäller att hantera informationssäkerhet kopplat till användandet av mobila enheter står helt klart. Ett av problemen ligger i att företagen har väldigt svårt att veta var informationen finns och hur informationen ska skyddas när den är utanför företagets domäner. Ett annat problem är hur de ska skydda sina mobila enheter från skadlig kod, obehörig fysisk access och att enheten tappas bort, blir stulen vilket i sin tur kan leda till att information hamnar i fel händer. En liten lösning av problematiken tycks ligga i att etablera säkerhetspolicys inom företaget och att försäkra sig om att användarna har förstått dessa. Organisationer måste genomföra utbildning inom informationssäkerhet för sina anställda, hur de arbetar på ett säkert sätt. En annan del av lösning är att implementera lager-på-lagersäkerhet och se till att ha uppdaterad mjukvara för att minimera risken för skador.

3.2 Basnivå för informationssäkerhet, BITS

BITS är en samling rekommendationer från Krisberedskapsmyndigheten (KBS), i rekommendationerna specificeras en lägsta nivå för informationssäkerhet i organisationer, basnivå. BITS innehåller ett stort antal administrativa säkerhetsåtgärder som minst måste utföras för att en organisation ska uppnå en acceptabel säkerhetsnivå. BITS är utformad efter att passa den svenska säkerhetsstandarden SS-ISO/IEC 17799. BITS kom i en ny och reviderad version i början av 2006.

Arbetsprocessen som BITS utgår från är uppdelad i fyra steg. 1, Organisationen definierar mål och inriktning för säkerhetsarbetet genom att ta fram en informationssäkerhetspolicy, ett övergripande dokument för att styra informationssäkerhetsarbetet. 2, Informationssäkerhetspolicy realiseras i säkerhetsinstruktioner för användare, för kontinuitet och drift, samt för personal på en administrativ och förvaltningsnivå. 3, Med informationssäkerhetspolicyn som bas görs en systemsäkerhetsanalys för varje informationssystem av betydelse, kraven utgår från aspekterna sekretess, riktighet och tillgänglighet. Skulle kraven överstiga basnivån i BITS behövs kompletterande säkerhetsarbete. 4, Man bedömer de genomförda säkerhetsåtgärderna och hur utfallet blivit om det behövs mer åtgärder etcetera, en säkerhetsutvärdering tas fram som ligger till grund för ett beslut om driftgodkännande.

Utgångspunkten för arbetet ska vara att man genomför risk- och sårbarhetsanalyser för att få möjlighet att klarlägga vilken säkerhetsnivå som organisationen behöver, BITS ska endast ses som

en lägstanivå som inte får underskridas och det är möjligt att verksamheten kräver en högre säkerhetsnivå. Vår undersökning riktar endast in sig på de punkter vi finner centrala i BITS i förhållande till våra frågeställningar. Med systemägare syftar vi på den person i organisationen som ansvarar för anskaffning, förvaltning, användning och säkerhet av ett informationssystem.

3.2.1 Säkerhetspolicy

Mål: ”Att ange ledningens viljeinriktning och stöd för informationssäkerhet i enlighet med organisationens verksamhetskrav och relevanta lagar och föreskrifter.” (Krisberedskapsmyndigheten, 2006, s.13)

Det är ledningen som fastställer informationssäkerhetspolicyn och ansvarar för att policyn är dokumenterad, att all personal får information om innehållet, de ansvarar även för att kontinuerligt granska säkerhetspolicyn. Policyn ska uttrycka ledningens engagemang, definition, omfattning och vikten av informationssäkerhet. Den ska även innehålla de mål och metoder företaget har till förfogande för att styra arbetsprocessen samt utrycka strukturer för riskbedömning och riskhantering. Säkerhetspolicyn ska beskriva långsiktiga mål för informationssäkerhetsarbetet, organisation, roller och dess ansvar för informationssäkerhetsarbetet. Den ska även vara kortfattad och lätt att förstå för de anställda.

3.2.2 Organisation av informationssäkerheten

Mål: ”Att hantera informationssäkerhet inom organisationen.” (Krisberedskapsmyndigheten, 2006, s.15)

Ledningen ska tillgodose behovet av resurser för informationssäkerhet. Den ska besluta hur arbetet med informationssäkerhet ska bedrivas i praktiken i form av mål, organisation, ansvar och roller. Det är även ledningens ansvar att identifiera förändringar av hotbilden för att kunna genomföra åtgärder, samt identifiera eventuellt behov av att anlita rådgivare, exempelvis säkerhetsexperter. Det är i denna punkt organisationens ledning ska säkerställa att de åtgärder för informationssäkerhet som tas i bruk samordnas i alla delar av organisationen.

I denna kategori ska det försäkras att det finns instruktioner gällandes informationssäkerheten för förvaltning, för användare samt för kontinuitet och drift. Ledningen ska också besluta om en informationssäkerhetssamordnare och denna ska direkt vara underställd organisationens chef. Samordnaren ska samordna säkerhetsarbetet inom organisationen, medverka i framtagning av styrdokument, systemsäkerhetsanalyser, säkerhetsinstruktioner och informationssäkerhetspolicyn. Samordnaren ska också ha rollen som informatör och rådgivare i informationssäkerhetsfrågor, och medverka i genomförandet av olika säkerhetsrelaterade åtgärder, det ligger också på samordnarens roll att följa upp att de specificerade säkerhetsinstruktionerna efterföljs i organisationen. Det är också dennes ansvar att delta i framtagandet av generella rutiner gällandes informationssäkerhet inom organisationen, exempelvis rutiner för incidenthantering.

Man ska skapa en systemförteckning där man identifierar och förtecknar samtliga informationssystem organisationen använder sig av, det ska i denna företeckning även framgå vilka av dessa system som är centrala för verksamheten. Varje informationssystem ska ha en egen systemsäkerhetsanalys och dessa systemsäkerhetsanalyser måste revideras om det sker större förändringar av verksamhetens inriktning, förändringar i hotbilden etcetera.

Inom vissa områden i organisationens verksamhet kan det finnas behov för framtagandet av speciella regler, exempelvis vad som ska gälla vid distansarbete och uppkoppling mot organisationens nät utifrån. Organisationen måste också specificera upp vad som gäller för information och resurser som är åtkomlig, bearbetas, kommuniceras till eller styrs av utomstående parter. BITS kräver att det finns dokumenterade regler vid åtkomst till information eller informationssystem av en från organisationen utomstående aktör, konsulter, servicepersonal etcetera.

3.2.3 Hantering av tillgångar

3.2.3.1 Ansvar för tillgångar

Mål: ”Att uppnå och upprätthålla lämpligt skydd av organisationens tillgångar.” (Krisberedskapsmyndigheten 2006, s.19)

Tillgångar specificeras enligt BITS i tre kategorier. Informationstillgångar som är databaser, datafiler, systemdokumentation, användarmanualer, utbildningsmaterial, administrativa rutier, drift- och servicerutiner, kontinuitetsplaner, avbrottsplaner och arkiverad information. Programtillgångar som specificeras som tillämpningsprogram, nätverk- och operativsystem samt utvecklingsverktyg. Fysiska tillgångar som inkluderar all hårdvara såsom datorer, kommunikationsutrustning, lagringsmedia och annan teknisk utrustning. För att uppnå basnivå måste det finnas en ansvarsfördelning för samtliga informationstillgångar inom organisationen, omflyttning eller överlåtelse av informationsutrustning ska ske enligt specificerade rutiner. Organisationen ska även ha framtagna regler för hur informationsbehandlingsresurser får användas.

3.2.3.2 Klassificering av information

Mål: ”Att säkerställa att informationstillgångar får en lämplig skyddsnivå.” (Krisberedskapsmyndigheten, 2006, s.20)

För att basnivå ska uppnås ska organisationen uppfylla fyra kriterier. Det ska finnas regler för klassning av information. Information som behandlas ska klassificeras med hänsyn till krav på skyddsnivå. Det är systemägaren det vill säga han som ansvarar för informationssystem, som är ansvarig för att klassificeringen genomförs och säkerställer att säkerhetskraven tillgodoses. Organisationen måste även ha tagit fram regler för hur datamedia ska klassas och hur datamedia ska märkas och förtecknas. På lagringsmedia såsom hårddiskar kan information där klassningsgraden skiljer sig förekomma, det är därför viktigt att datamedia även omfattas av klassning. Avsikten med denna märkning och förteckning är att datamedia inte ska förväxlas, märkning och förteckning ska även gälla säkerhetskopior. För att förhindra att klassificering av information inte görs slentrianmässigt menar BITS att man ska genomföra utbildning i hur klassificering ska genomföras med viss regelbundenhet, förslagsvis vartannat år. Nyanställda ska gå utbildning i regler och rutiner gällandes informationsklassning innan de ges behörighet till informationssystemen i fråga.

3.2.4 Personalresurser och säkerhet

3.2.4.1 Före anställning

Mål: ”Att säkerställa att anställda, leverantörer och utomstående användare förstår sitt ansvar och är lämpliga för de roller de avses ha och för att minska risken för stöld, bedrägeri eller missbruk av resurser.” (Krisberedskapsmyndigheten 2006, s.21)

För att uppnå basnivå ska organisationen fastställa tre delpunkter. Vid nyanställning ska en kontroll göras av personens bakgrund i förhållande till kommande arbetsuppgifter. Det ska ligga på chefer i linjeorganisationen att ansvara för att medarbetare och inhyrd personal får information om säkerhetspolicyn och instruktioner som personerna i fråga kan tänkas vara i behov av. Det är systemägarens ansvar att definiera vilka krav som ska ställas på användare som ska få tillgång till informationssystemet, kraven ska vara dokumenterade och avse såväl säkerhet som kompetens.

3.2.4.1 Under anställning

Mål: ”Att säkerställa att anställda, leverantörer och utomstående användare är medvetna om hot och problem som rör informationssäkerhet, sitt ansvar och sina skyldigheter samt är utrustade för att stödja organisationens säkerhetspolicy när de utför sitt normala arbete och att minska risken för mänskliga fel.” (Krisberedskapsmyndigheten, 2006, s.22)

Det finns tre grundkrav för att uppnå basnivå, dokumenterade och av ledningen beslutade säkerhetsinstruktioner för användare, organisationen ska regelbundet genomföra utbildning inom informationssäkerhetsrelaterade frågor, och det ska finnas användarhandledning för varje informationssystem. Säkerhetsinstruktionen ska redovisa generella informationssäkerhetsregler inom organisationen, hur personalen hanterar organisationens informationssystem och övriga IT-resurser. Som några exempel kan nämnas regler för hur dokument ska framtas, hur de ska klassificeras, hur användaren ska hantera e-post och hur användaren får använda Internet. BITS poängterar vikten av kontinuerlig utbildning inom informationssäkerhet för de anställda, dels för att försäkra om att kunskapen om informationssäkerhet ska vara tillfredställande men även för att bibehålla motivation samt högt säkerhetsmedvetande hos de anställda.

En användarhandledning för ett informationssystem ska skapas. Den ska minst innehålla en övergripande beskrivning, hur användaren ska arbeta med systemet, vart man ska vända sig om problem med systemet inträffar (incidentrapporter etcetera), säkerhetsbestämmelser för systemet och informationen lagrad i detta, eventuella rutiner för utlämning av information.

3.2.4.1 Avslutande av anställning eller förflyttning

Mål: ”Att säkerställa att anställda, leverantörer och utomstående användare lämnar organisationen eller ändrar anställningsförhållande på ett ordnat sätt.” (Krisberedskapsmyndigheten, 2006, s.23)

För att uppnå basnivå ska för anställda, leverantörer och utomstående användare gälla att alla tillgångar som tillhör organisationen återlämnas, åtkomsträtten till information eller informationsbehandlingsresurser ska tas bort.

3.2.5 Fysisk och miljörelaterad säkerhet

3.2.5.1 Skydd av utrustning

Mål: ”Att förhindra förlust, skada, stöld eller skadlig påverkan på tillgångar och avbrott i organisationens verksamhet.” (Krisberedskapsmyndigheten, 2006, s.25)

För basnivå krävs det att när man ska ta utrustning som lagrar känslig information ur bruk ska informationen raderas på ett säkert sätt, BITS menar även att stöldproblematiken när det kommer till mobila enheter ska beaktas. Beroende på informationen som den mobila enheten ska hantera kan särskilda säkerhetsåtgärder behöva implementeras. Vid exempelvis distansarbete ska man ha samma krav på säkerhetsskyddet på den arbetsplatsen som man har för arbetsplatsen inom organisationen. Ska man uppnå basnivå ska all utrustning och information som ska föras ut från organisationens lokaler få ett godkännande av ansvarig chef, ibland kan det enligt BITS vara motiverat med rutiner som hanterar utförsel och kvittering.

3.2.6 Styrning av kommunikation och drift

3.2.6.1 Driftrutiner och driftansvar

Mål: ”Att säkerställa korrekt och säker drift av informationsbehandlingsutrustning.” (Krisberedskapsmyndigheten, 2006, s.27)

För att organisationen ska uppnå basnivå krävs att ledningen har tagit fram säkerhetsinstruktioner för drift, som minst omfattar säkerhetskopiering, återstarts- och återställningsrutiner samt hantering av revisioner och logginformation.

3.2.6.3 Skydd mot skadlig och mobil kod

Mål: ”Att skydda riktighet i program och data.” (Krisberedskapsmyndigheten, 2006, s.32)

För att man ska uppnå basnivå ska det finnas rutiner framtagna för skydd mot skadlig programkod. Minimumkrav är att skydden ska detektera förekomst av skadlig kod, rutiner ska finnas för att kontinuerligt installera nya uppdateringar av skydden, både på servrar och klienter. Uppdatering av skydden gäller både för operativsystem och applikationsprogram och rutinerna för dessa uppdateringar ska om möjligt vara automatiserade. En annan punkt som krävs för basnivå är att skyddet alltid ska starta automatiskt när en dator startas, ett aktivt skydd. Men en organisation kan också använda sig av passiva skydd för ett extra skydd. Ett passivt skydd går vid vissa speciella tidpunkter in i organisationens nätverk och letar efter virus, onormal aktivitet etcetera.

För basnivå ska också användares rätt att installera program och import av externa filer regleras och finnas väl dokumenterade i en säkerhetsinstruktion för användare, detta är enligt BITS en viktig del av skyddet, att kunna kontrollera vilka program som får köras i informationssystemet och på vilket sätt information får tillföras informationssystemet, just det faktum att så många är anslutna till Internet belyser riskerna med denna problematik.

Mobilkod är ett litet program som överförs mellan datorer och exekveras automatiskt, det kan finnas i bilagor i e-post som innehåller mobilkod, men även vanliga Internetapplikationer såsom Internetbanker kan använda sig av denna typ av kod. Några risker med mobilkod är att det kan användas för att stjäla eller manipulera information. Om företaget godkänner att användarna får köra mobilkod ska regler finnas för detta som reglerar hur, när och vilken mobilkod som användarna får köra.

BITS poängterar dock att skyddet mot skadlig programkod ska stå i relation till eventuella skador ett angrepp kan orsaka, aktuella åtgärder som kan genomföras är åtgärder som bidrar till att upptäcka, förebygga, förhindra smittspridning samt återställa smittat system. Ett alternativ är att dela upp organisationens nätverk i mindre enheter med hjälp av segmentering, för att se till att en attack endast drabbar en mindre del av nätverket, organisationer bör också överväga att filtrera Internettrafiken.

3.2.6.3 Säkerhetskopiering

Mål: ”Att bevara informationens och informationsbehandlingsresursernas riktighet och tillgänglighet.” (Krisberedskapsmyndigheten, 2006, s.33)

Säkerhetskopiering ska genomföras regelbundet och det är systemägarens ansvar att besluta om tidpunkt och dokumentering där han beskriver intervall, vilket information som ska omfattas, hur säkerhetskopiorna ska förvaras, hur ska man kunna försäkra sig om kvalitet på säkerhetskopiorna. Dokumenteringen mynnar ut i något som i BITS kallas för Säkerhetsinstruktion, kontinuitet och drift, där det även ska finnas beskrivet hur man ska testa att informationssystemet kan återställas utifrån säkerhetskopiorna och hur ofta sådana tester ska genomföras, BITS rekommendationer är att det minst ska göras årligen.

3.2.6.4 Hantering av media

Mål: ”Att förhindra obehörigt avslöjande, modifiering, borttagning eller förstörande av tillgångar och avbrott i organisationens verksamhet.” (Krisberedskapsmyndigheten, 2006, s.36)

Återigen krävs klassificering av informationen för att kunna avgöra vilka datamedia som ska skyddas mot obehörig åtkomst. Om datamedia transporteras utanför organisationen ska klassificeringen av informationen på denna avgöra om man ska kryptera innehållet och elektroniskt signera det. Flyttbara media som lämnar organisationen ska förtecknas för få spårbarhet. Information som finns på flyttbara media och som inte längre behövs ska överskrivas med teknik som motsvarar klassificeringsgraden av informationen.

3.2.6.5 Utbyte av information

Mål: ”Att bibehålla säkerheten hos information och programvara som utbyts inom organisationen och med någon extern enhet.” (Krisberedskapsmyndigheten, 2006, s.38)

För basnivå krävs att regler för vilken information som får skickas med e-post finns dokumenterade i säkerhetsinstruktion för användare. Det måste även finnas viruskontroll för e-postmeddelanden och eventuella bifogade filer. Reglerna för e-post ska utgå från informationens klassificering, och förklara vilken typ av information som ska krypteras och eventuellt ha en

elektronisk underskrift. Om en användare skulle bli smittad av virus via ett e-postmeddelande ska kontakt tas med ansvarig, vidare ska försiktighet vara ledordet vid öppnandet av bifogade filer.

3.2.7 Styrning av åtkomst

3.2.7.1 Verksamhetskrav på styrning av åtkomst

Mål: ”Att styra åtkomst till information.” (Krisberedskapsmyndigheten, 2006, s.44)

För basnivå ska systemägaren fastställa vilka och vilken typ av anslutningar till tele- och datanät som ska vara tillåtna, om möjligt ska användaren endast ha rättigheter som är tillräckliga för att han ska kunna utföra sina arbetsuppgifter via exempelvis ett behörighetskontrollsystem. Ett behörighetskontrollsystem möjliggör identifiering av en användaridentitet , att användaren inte har rättighet till informationssystem denne inte ska ha tillgång till, det ger också organisationen möjlighet att registrera alla aktiviteter användaren utför i informationssystemen. Med behörighet menas det i BITS en användares rättighet att på ett reglerat sätt utnyttja ett informationssystem och dess resurser. Om man vill uppnå en bra lösning på behörighetsproblematiken krävs flertalet tekniska och administrativa åtgärder, ett behörighetskontrollsystem kräver också både administrativa och tekniska åtgärder.

Det ligger på systemägarens ansvar att se till att dessa behörighetsregister som skapas endast är åtkomliga för en utsedd administratör, en administratör som också är den som har rättighet att registrera, förändra eller ta bort en användares åtkomsträttigheter. Minst en gång om året ska det kontrolleras att endast behöriga användare är registrerade i behörighetssystemet..

3.2.7.2 Styrning av användares åtkomst

Mål: ”Att säkerställa behörig användares åtkomst och förhindra obehörig åtkomst till informationssystem.” (Krisberedskapsmyndigheten, 2006, s.44)

Ett annat problem som kan uppstå är när personer lämnar sina arbetsstationer utan att logga ut eller de glömmer att låsa sin arbetsstation. Viktigt att poängtera att vid användning av mobila enheter är det en punkt som måste ses över ytterligare då enheten ofta befinner sig i en miljö utanför företaget. En extra åtgärd som krävs för basnivå är att införa en centralt styrd tidsperiod för automatisk aktivering av exempelvis skärmsläckare, för att komma in i systemet igen måste användaren på nytt skriva in sitt lösenord. Det poängteras även att användare inte bör ha rättighet till att installera program på sin arbetsstation, att han inte ska ha åtkomst till operativsysteminställningar eller systemverktyg, program ska endast få installeras av användare med speciellt utsedd behörighet.

BITS specificerar upp klara regler för lösenord, ett lösenord ska bestå av minst åtta tecken och vara konstruerade så att de inte lätt går att pröva sig eller gissa sig fram till det, vidare ska endast användaren känna till lösenordet och endast han ska ha rättighet till att ändra det. En användare ska även tvingas byta lösenord efter ett tidsintervall som beslutas av systemägaren, och ett användarkonto ska låsas efter tre felaktiga inloggningsförsök, för basnivå ska ett lösenord inte kunna återanvändas på minst tretton månader.

På en administrativ nivå ska man se till att antalet konton med privilegierade rättigheter begränsas, det ska även finnas framtagna rutiner för hur man hanterar behörighet för en anställd

som slutar eller byter arbetsuppgifter. När en användare får behörighet ska denne informeras om de generella säkerhetsinstruktioner och regler som gäller för organisationen, men även specifika instruktioner kopplade till användarens arbetsuppgifter.

3.2.7.3 Användares ansvar

Mål: ”Att förhindra obehörig användaråtkomst och åverkan eller stöld av information och informationsbehandlingsresurser.” (Krisberedskapsmyndigheten, 2006, s.47)

En användare ska skydda sitt lösenord väl och byta det vid första misstanke om att någon annan känner till det, användaren får inte heller låna ut sin behörighet till andra. Det finns även en risk med i och med att om användaren använder samma lösenord utanför organisationen, om lösenordet skulle komma i orätta händer och användaren skulle gå att spåra till sin arbetsplats finns det genast en ökad risk för obehörig åtkomst. Användaren ska enligt BITS följa de uppsatta reglerna och vara noga med att hantera sitt lösenord säkert.

3.2.7.4 Styrning av åtkomst till nätverk

Mål: ”Att förhindra obehörig åtkomst till nätverkstjänster.” (Krisberedskapsmyndigheten, 2006, s.48)

Styrning av åtkomst till nätverk är del av BITS som behandlar brandväggar. Brandväggen ska vara den enda kanalen för ingående och utgående IP-baserad datakommunikation hos organisationen, och för att uppnå basnivå ska brandväggen även ha skydd mot skadlig programkod Om trådlösa nätverk används inom organisationen är det nätverkets systemägare som ska besluta om åtgärder för att förhindra obehörig avlyssning samt nyttjande. BITS nämner att allt fler organisationer bygger upp trådlösa nät inom organisationen med hjälp av WLAN (Wireless Local Area Net), då tillför man problematik genom att inte endast vara i behov av att autentisera klienter, utan även av att autentisera infrastrukturen.

Enligt BITS är det inte tillräckligt att använda sig av Wired Equivalent Privacy (WEP) som är en säkerhetslösning som omfattar autentisering, kryptering och integritetskontroll, man bör enligt BITS kombinera WEP med andra säkerhetslösningar. Så kallade accesspunkter i trådlösa nät ska stängas av under de perioder de inte används. Behöver information nås utifrån ska behovet av rätt autentiseringsmetod utredas, det ska även finnas regler för hur autentisering ska ske via externa anslutningar. Dessa regler specificeras i säkerhetsinstruktion förvaltning. Där ska även anvisningar för säkerhet vid Internetanslutningar finnas uppsatta, och uppkoppling mot Internet får endast ske om säkerhetsfunktionerna är igång.

3.2.7.5 Styrning av åtkomst till information och tillämpningar

Mål: ”Att förhindra obehörig åtkomst av information i tillämpningar.”
(Krisberedskapsmyndigheten, 2006, s.51)

För basnivå krävs att det finns tydligt uppsatta regler för åtkomst av information. En grundregel är att åtkomst ska begränsas i förhållande till behovet användaren har för att kunna utföra sitt arbete. Man bör även se till att användare med bärbara datorer har som skyldighet att se till att för organisationen viktig data kopieras in på någon form av backup. Behörighetssystemet ska konstrueras så att behörighet knyts till användarnas identitet

3.2.7.6 Mobil datoranvändning och distansarbete

Mål: ”Att säkerställa informationssäkerheten vid användning av mobil utrustning och utrustning för distansarbete.” (Krisberedskapsmyndigheten, 2006, s.52)

Kraven för basnivå är att kraven på säkerhet och den praktiska hanteringen av mobila enheter är dokumenterade i säkerhetsinstruktion, användare. Det är sedan upp till systemägaren att ge användare tillstånd om informationen i aktuellt system ska få bearbetas på distans eller med mobila enheter. BITS menar att det kan finnas behov av att vara extra försiktig när det gäller arbete med mobila enheter utanför organisationen, exempelvis distansarbete. Frågor som kan tänkas behöva behandlas är huruvida obehörig användning av hårdvara kan ske, säkerhetskopiering, kontroll av skadlig kod, kryptering och autentisering vid kommunikation mot arbetsplatsen. Ibland kan det finnas skäl att ha kontroll av klienter innan de kommer in på företagets nätverk, att man försäkrar att de har rätt säkerhetspatchar och uppdaterade antivirusprogram.

3.2.8 Anskaffning, utveckling och underhåll av informationssystem

3.2.8.1 Kryptering

Mål: ”Att skydda informationens sekretess, autenticitet eller riktighet med kryptering.” (Krisberedskapsmyndigheten, 2006, s.56)

Enligt BITS bör kryptering användas inom organisationen samt vid externa uppkopplingar till och från dess nät ifall klassificering av informationen ställer höga krav på skydd mot obehörig avlyssning, insyn och förändring, men även då man är i behov av elektroniska underskrifter samt säker autentisering. Behovet av kryptering ska grundas på riskanalyser och krävs kryptering ska regler för det dokumenteras i säkerhetsinstruktion, förvaltning.

3.2.9 Hantering av informationssäkerhetsincidenter

3.2.9.1 Rapportering av säkerhetshändelser och svagheter

Mål: ”Att säkerställa att informationssäkerhetsincidenter och svagheter hos informationssystem rapporteras på ett sådant sätt att korrigerande åtgärder kan vidtas i rätt tid.” (Krisberedskapsmyndigheten, 2006, s.62)

För basnivå krävs fastlagda rutiner för hur användare ska agera vid misstanke om intrång, funktionsfel samt andra störningar. Detta ska dokumenteras i säkerhetsinstruktion, användare.

3.2.9.2 Hantering av informationssäkerhetsincidenter och förbättringar

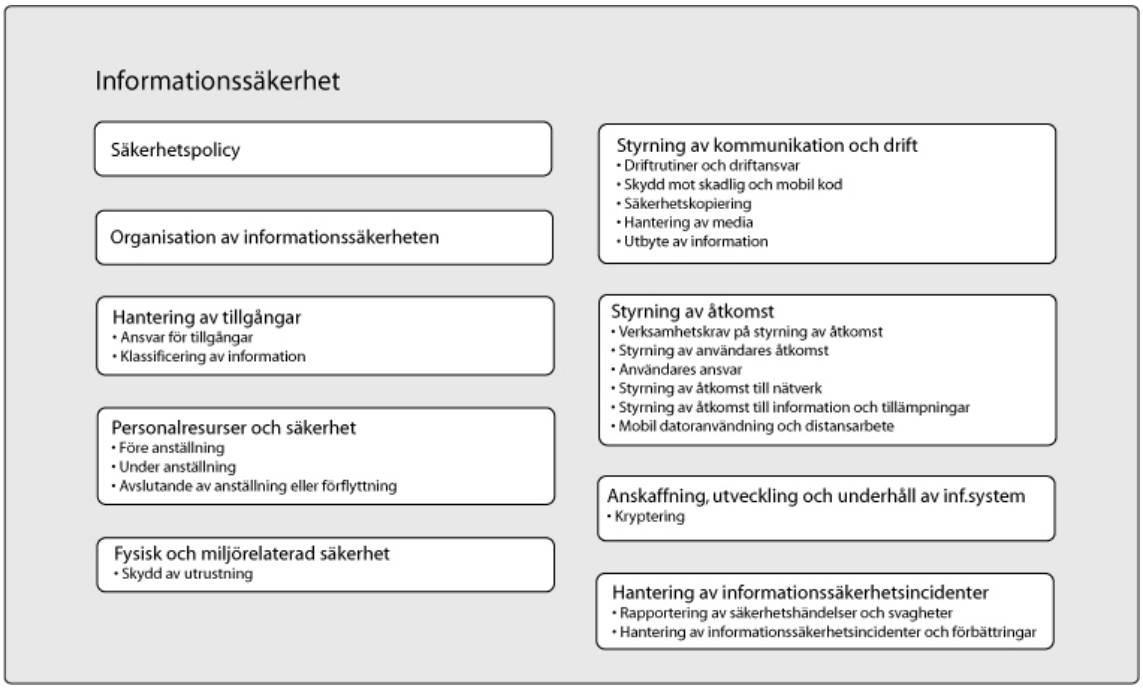
Mål: ”Att säkerställa att ett konsekvent och effektivt angreppssätt tillämpas på hanteringen av informationssäkerhetsincidenter.” (Krisberedskapsmyndigheten, 2006, s.69)

Det ska för basnivå finnas rutiner för hur uppföljning av det användarna rapporterar ska skötas, dokumenterat i säkerhetsinstruktion, förvaltning. BITS menar att möjligheten att återkoppla

erfarenheter från incidenter är av central betydelse för att kunna spåra svagheter och andra brister i informationssäkerheten.

4 Undersökning

Vi valde BITS som grund för vår undersökning och tog fram en modell för informationssäkerhet baserad på BITS och de delar vi fann centrala utifrån våra frågeställningar. Varför BITS valdes är för att det är de absolut minsta kraven för informationssäkerhet enligt Krisberedskapsmyndigheten. BITS har implementerats i de flesta svenska kommuner och i alla svenska länsstyrelser och bör således även stödja användandet av mobila enheter. Då det framkommit tidigare att användandet av mobila enheter och tekniker samt trender kopplat till det fortsätter att öka är det av stor vikt att BITS hanterar detta.



Figur 4.1. Undersökningsmodell för informationssäkerhet vid användande av mobila enheter, modell baserad på BITS.

Expertintervjuerna och informationen som framkom efter kodningen av dessa ställdes mot modellen. Vi jämförde vad informanterna poängterade mot vad respektive BITS-kategori menar. Experterna vi intervjuade var Magnus Lindkvist, Cheif Security Advisor på Microsoft AB, Per Hellqvist, säkerhetsexpert på Symantec Nordic AB samt Johan Jarl, säkerhetsexpert på F-Secure. Intervjuerna genomfördes efter en semistrukturerad form med ämnesområden med delkategorier som skulle behandlas under intervjun. Ämnesområdena återfinns i bilaga 2, Expertintervjuer, ämnesområden.

4.1 Informationssäkerhetspolicy

> ”Men de anställda måste förstå vilka regler och riktlinjer som finns i företaget, så det är egentligen företaget som har det största ansvaret att se till att de anställda har läst och förstått policyn, inte bara läst den.” Per Hellqvist, Symantec

Att en informationssäkerhetspolicy är en av de viktigaste punkterna när det kommer till informationssäkerhet var Per och Magnus överens om. Enligt Per Hellqvist är en punkt som företag slarvar med den att kontrollera förståelsen av policyn hos användarna. Om företaget har kommunicerat ut förändringar i sin policy till sina anställda behövs det verktyg för att kunna konfirmera att de verkligen har förstått vad som har förändrats. Han menar även att det är av central betydelse att i policyn specificera hur organisationen kommer att reagera om någon anställd bryter mot policyn. Eller om det sker någon annan form av incident orsakad av att en anställd inte har följt den uppsatta policyn. Om man inte går ut och berättar vad som kommer betraktas som en incident och vad följderna blir, då kommer de anställda att kunna hävda att de inte har fått information om detta och organisationen kommer inte att kunna komma till bukt med problemen enligt Per. Vidare menade han att det inte är sällsynt att policyn inte är förankrad i verksamheten, ansvarig för policyn har suttit på sin kammare och skrivit en policy enligt böcker och best practices, men han har inte pratat med organisationen. Johan Jarl påpekade också problemet med att det väldigt ofta är en ensam person som utan att kontrollera verksamheten skapar en säkerhetspolicy. En policy som upphovsmannen sedan antar att alla ska följa, utan att försäkra sig om att de anställda har läst och förstått den.

> ”Man måste komma ihåg det att det är IT-säkerheten som är verksamhetsstyrd, det är verksamheten som har mål och visioner som IT-säkerheten skall stödja, inte tvärtom.” Per Hellqvist, Symantec

Policyn och hur företaget arbetat med informationssäkerhet påverkar ju i stor grad alla anställdas sätt att arbeta, om man i ledningen inte har fått feedback från de anställda och korrigerat ramen för informationssäkerhetsarbetet kan man få problem med det dagliga arbetet inom organisationen enligt Per. Detta belyser vikten av att granska säkerhetspolicyn för att kunna utvärdera och få möjlighet till att kunna se hur den är förankrad i organisationen vilket även BITS belyser i målbeskrivningen av Informationssäkerhetspolicy.

Magnus Lindkvist menade att det är ledningens yttersta ansvar att se till att en informationssäkerhetspolicy kommer till stånd, det är ledningen som har det ultimata ansvaret för informationssäkerheten. Just vikten av en policy belyses då man enligt Magnus inte enbart kan arbeta med tekniska lösningar för att komma till bukt med informationssäkerhetsfrågor.

> ”Om det inte finns en policy i företaget, ett tydligt regelverk för vad som gäller kan du göra hur mycket som helst på tekniksidan” Magnus Lindkvist, Microsoft AB

Precis som BITS nämner samtliga informanter att det är viktigt att policyn är kortfattad, övergripande och lätt att förstå, Magnus och Johan nämner att den ska få plats på en sida. BITS poängterar att man kontinuerligt ska granska sin säkerhetspolicy och att det är lednings ansvar, vilket får starkt stöd hos våra informanter. Men i BITS är det oklart vad granska har för innebörd. Våra informanter poängterar flertalet gånger att det är av stor betydelse att följa upp och försäkra sig om att policyn har blivit etablerad hos, samt förstådd av de anställda vilket inte BITS gör i speciellt stor utsträckning.

4.2 Organisation av informationssäkerheten

Inom denna kategori fick vi inte speciellt mycket information från våra informanter. Den samordnande rollen tas oftast av IT-chef eller dylik enligt dem, Per poängterande precis som BITS att det är samordnares roll att vara en form av omvärldsbevakare. Omvärldsbevakare när det gäller skadlig kod och nya sårbarheter i mjukvara som finns inom organisationen, och det ligger på dennes ansvar se till att organisationen är rustad för nya hot. Även Johan poängterade vikten av att man genomför omvärldsbevakning om man har ansvar för informationssäkerheten i ett företag.

> ”Från dag till dag kan allting förändras så att man måste hela tiden omvärldsbevaka och utbilda användarna.” Johan Jarl, F-Secure

Magnus ger stöd för riktlinjerna i BITS som handlar om systemförteckning och varje informationssystems systemsäkerhetsanalys, detta behövs för att kunna nå något som han kallar för ”rätt säkerhet” för varje situation och informationssystem.

> ”Rätt säkerhet, det får man endast om du har satt dig ner och funderat på, vad är det jag vill skydda, hur mycket är den data jag vill skydda värd, vad händer om fel personer då får tag på det data jag försöker skydda?” Magnus Lindkvist, Microsoft AB

Först när man har gjort detta kan man förstå vilka metoder man vill använda för att skydda sig, vilka resurser ska läggas för att skydda informationen i den aktuella kontexten, han belyser det med att förklara att det är skillnad på att sitta på ett nätverk med nästan enbart publik information och Microsofts interna nätverk där det finns stora mänger konfidentiell information.

BITS nämner kortfattat att det kan finnas behov för framtagandet av regler och policys för områden som distansarbete och uppkoppling mot organisationens nät utifrån. Enligt Per har organisationer inte riktigt fått in mobilitet i sina policys och regler, vilket är ett problem enligt honom. De anställda vet inte hur de ska hantera informationssäkerhet när det kommer till mobila enheter, de vet helt enkelt inte riskerna och hur de ska bete sig menar han, man måste utbilda användarna i informationssäkerhet kopplat till mobilitet. Johan var av åsikten att det måste finnas en klar och tydlig policy. En policy som informerar användarna om vad som gäller vid distansarbete från hemmet och för användandet av bärbara datorer rent allmänt.

4.3 Hantering av tillgångar

För kategorin ansvar för tillgångar kom informanterna mestadels med synpunkter gällandes informationstillgångar, vilket är också den av betydelse när det gäller riskerna med mobila enheter, Magnus påpekade att kostnaden för hårdvara täcks av försäkringar, men informationen som kan komma i fel händer kan kosta betydligt mer.

> ”Men det skulle vara ett större problem om jag hade hela källkoden för nästa operativsystem på min laptop, och de kunde sälja den för x antal miljoner kronor till en konkurrent.” Magnus Lindkvist, Microsoft AB

Problemen är att när det gäller informationstillgångar är det väldigt svårt att ha spårbarhet på dessa, i dagsläget är det väldigt lätt för information att lämna organisationen, framför allt när det gäller digitala informationstillgångar förklarade Magnus. Det var också det som Microsoft fick

mycket förfrågningar om, hur kan jag följa upp vart vår information finns någonstans? För att komma till bukt med denna problematik var han av åsikten att det är genom policys och riktlinjer man får möjlighet att förankra hur man får behandla olika typer av informationstillgångar, beroende på klassificeringen av den aktuella informationen. Per vidhöll också att detta är ett jätteproblem hos organisationer.

> ”Problemet idag är ju att alla som arbetar med IT-säkerhet och informationsfrågor behöver ju veta vart informationen finns vid varje givet tillfälle.” Per Hellquist, Symantec

Per menade att det faktum att man flyttar information hela tiden, man synkar sin e-post mot sin mobiltelefon och sedan rör sig ut från företaget med informationstillgångarna i mobiltelefonen, idag är detta ett enormt svart hål för den som skall skydda informationen. Idag är det väldigt svårt att kontrollera vilken information som finns på vilken enhet, det går via loggar och etcetera men det är oerhört svårt förklarade han.

Klassificering av information är en av grundpelarna i informationssäkerhetsarbete enligt Per och Magnus. De båda delade upp information i tre kategorier, publik, intern och hemlig. Publik information som är tillgänglig för alla, information som inte innebär några risker för företaget. Intern information ska stanna inom organisationen, och hemlig information innebär att endast en begränsad grupp inom organisationen ska ha tillgång till det. Ibland kan det även finnas behov av en konfidentiell klassificerings kategori enligt Magnus.

Per berättade att företag generellt sett slutade med att klassificera information för flera år sedan, vilket leder till att de inte vet vilken information som är hemlig och vilken som är publik. Vilket i slutändan leder till att det är chans att anställda skickar ut hemlig information, vilket uppenbart är ett problem. För basnivå kräver BITS att det ska finnas dokumenterade regler för klassning av information vilket får mycket starkt stöd hos Per och Magnus.

> ”om jag inte vet hur jag ska klassa min information kan inte bestämma hur jag ska skydda den” Magnus Lindkvist, Microsoft AB

Problemen är enligt Per att det inte finns något bra automatiskt sätt för att klassificera information, ingen automatik, vilket innebär att de anställda hela tiden själva måste ta ställning till hur de ska hantera och klassificera informationen. Anställda som sitter och jobbar med saker dag in och dag ut glömmer ganska lätt bort att tänka på klassificeringen av information, det är svårt att hålla disciplinen uppe.

Magnus berättade om att en del av problemen bottnar i att det inte går att lösa klassificeringsproblemet med enbart policys och rutiner eller enbart med teknik, utan det är en kombination av de båda som behövs för att nå bästa resultat. Ansvaret ligger således inte enbart på de anställda. En teknik som han berättade om var en av deras produkter för Rights Managment. Vilket innebär att så fort ett dokument eller liknande skapas så krypteras det och man kan sedan styra vilka som får öppna dokumentet via att man måste autentisera sig mot en server för att få rättighet att öppna dokumentet. Krypteringen följer med själva informationen och inte mediet det lagras på. BITS specificerar upp att det är systemägarens ansvar att hantera klassificeringen och se till att säkerhetskraven tillgodoses. Magnus var av åsikten att det är den som skapar informationen som bestämmer och ansvarar för vilken klassificering den skall ha, vilket går emot BITS som menar att det är den som äger ett informationssystem som ska ansvara för klassificeringen på information som finns på detta. Per menade att de som är ansvariga för

information ska klassificera denna, men ytterst ansvariga är ju ledningen trots allt menar han, klassificeringen ska specificeras i ett policydokument fortsätter han.

BITS är inte speciellt glasklar över hur informationstillgångar ska hanteras, framför allt när det kommer till elektroniska dokument som lätt lämnar organisationen via exempelvis e-post, något som också var ett stort problem enligt våra informanter. Mobila enheter såsom avancerade mobiltelefoner och bärbara datorer ställer problematiken med att hålla koll på vart information och hårdvara finns på högkant och BITS nämner inte någonting om detta i avsnittet om hantering av tillgångar.

4.4 Personalresurser och säkerhet

4.4.1 Under anställningen

Magnus belyste vikten av att enbart låta systemägaren eller annan utsedd person besluta om en person vid nyanställning (eller tilldelning av nya arbetsuppgifter) ska få tillgång till ett informationssystem eller inte. Enligt Magnus ligger det också på denna persons ansvar att informera användaren om de aktuella säkerhetsinstruktionerna och policys. Vid nyanställning ansåg Per att det var extra viktigt att följa upp att användaren verkligen har förstått innebörden och börjat arbeta efter den aktuella policyn. Detta för att personer som varit i organisationen under en längre tid troligtvis vet mer om företagets syn på informationssäkerhetsarbete. Något som inte BITS poängterar.

BITS målformulering för hantering av användare under anställningsperioden går till stor del ut på att säkerställa säkerhetsmedvetandet hos den anställde på flera olika plan. Magnus berättade om hur viktigt det är att kontinuerligt utbilda de anställda om hur och varför de ska arbeta med datorer på ett säkert sätt. Man kan förmana dem med policys och procedurer och ge dem tekniska hjälpmedel, men du måste hålla utbildning i incitament om varför de ska arbeta med datorn på ett säkert sätt. Ledningen måste fundera på vilka förutsättningar de ger sina användare att vara god medborgare i säkerhetsarbetet som han utryckte sig.

> ”Människans ansvar är så långt som någon har talat om för människan, man kan inte förvänta sig att alla personer tänker på samma sätt, och har samma bakgrund när det gäller informationssäkerhet.” Magnus Lindkvist, Microsoft

Men återigen poängterar han att enbart utbildning inte räcker speciellt långt. Säkerhet är som en kedja, man kan lägga resurser på en teknik men inget på utbildning, det fungerar inte. Man kan lägga allt på utbildning och inget på teknik, då riskerar du att användarna inte vet hur de ska använda systemet, eller så försöker de gå runt de säkerhetsinstruktioner och policys som finns, på grund av att de känner sig åsidosatta. En sådan enkel sak som lösenord, utbilda dina anställda i varför de ska välja ett starkt lösenord och inte låta andra få tag i det, har de inte kunskaperna om varför de ska arbeta säkert kommer de inte arbeta säkert ansåg Magnus. Johan ansåg att organisationen ska ha regelbundna möten med medarbetarna där de informerar om informationssäkerhet och hur man ska arbeta på ett säkert sätt.

Det är också väldigt viktigt för en organisation att presentera sina policys för sina anställda, för att hjälpa dem förstå hur de ska arbeta och varför de ska arbeta som policys föreskriver, men man får inte trycka ner dem i för mycket regler och rutiner ansåg Per. Magnus påpekade att det var viktigt att ta in åsikter från de anställda och utforma regler och policys som var enkla att ta till sig,

något som även Johan menade, och för att nå det ansåg han att policyn skulle vara lättillgänglig, kortfattad och enkel att ta till sig.

Alla informanterna poängterade om och om igen betydelsen av utbildning för informationssäkerheten. Det ena av Magnus tips till organisationer var bland annat att låta anställda få gå igenom olika policys med ansvarig person, och på det sättet få möjlighet att ge feedback, det andra tipset var att hålla utbildning för de anställda.

> ”Hur fungerar vår säkerhetspolicy? Har den ändrats eller uppdaterats? Utbildning ger incitament att till att få användare att bete sig på ett säkert sätt. Utbildning är en väldigt viktig del som en del ibland glömmer.” Magnus Lindkvist, Microsoft

Per var också av åsikten att utbildning av användare är centralt för att informationssäkerheten ska vara hög, men att det var ganska stort motstånd hos användarna att lära och ta till sig säkerhetsinstruktioner. Saker som att förbjuda användare att skicka roliga filer till varandra via e-post gör ju säkerhetsansvarige till killen som förstör festen, att arbeta med säkerhet är oftast väldigt otacksamt och det är lätt att bli hatad förklarade han. Vidare påpekade Per att det är väldigt viktigt att prata rätt språk med användarna, att inte bara förbjuda och låsa ner system utan även informera om varför man gör det, att försöka få en vikänsla inom företaget. BITS poängterar flertalet gånger behovet av och kravet på att utbilda användarna, men inte alls i lika stor utsträckning som våra informanter. Enligt Johan hade användarna ett stort ansvar i att arbeta säkert, de måste vara medvetna om de hot som existerar. De ska exempelvis vara uppmärksamma och inte öppna konstiga filer som de får skickade till sig via e-post förklarade han, något som han även pekade ut som ett stort problem ute i företag.

4.4.2 Avslutande av anställning eller förflyttning

När en anställning avslutas eller en anställd förflyttas ska man för basnivå se över och dra in eventuella rättigheter till system som den aktuella personen inte längre ska ha tillgång till, en människa ska ju inte ha tillgång till system han inte längre behöver ha tillgång till för att kunna utföra sina arbetsuppgifter. Det konfirmerades av båda våra informanter. Magnus ansåg att det var otroligt viktigt att ha policys och regler för hur man ska hantera anställda under och efter anställningen, vilket även BITS påpekar.

4.5 Fysisk och miljörelaterad säkerhet

4.5.1 Skydd av utrustning

Magnus nämnde att de större företagen oftast har en policy hur man skrotar hårdvara t.ex. hårddiskar. Klassificering av datamediet spelar stor roll eftersom om man jobbar med väldigt hemlig data är det ytterst viktigt att se till att informationen förstörs ifall man bestämmer sig för att skrota gammal hårdvara. Båda informanterna påpekade att många företag inte verkar har speciellt stor vetskap om att raderad information går att återställa med tekniska hjälpmedel

> ”Sen då kan man sätta en yxa i hårddisken för att avsluta det hela. Om man är riktigt paranoid så ska ju hårddisken malas ner till finspån.” Magnus Lindkvist, Microsoft AB

Återigen påpekade Magnus att de ekonomiska kostnaderna för att köpa in nya hårddiskar och liknande är i det långa loppet en ganska liten kostnad. I jämförelse med den kostnaden eller de risker som man får ifall informationen hamnar i fel händer. Men om man arbetar med publik data hela tiden är det inte lika angeläget att gå igenom samma nedrustningsprocess som om hårdvaran skulle innehålla intern eller hemlig data.

Magnus menade att det även måste gå att skydda informationen på mobiltelefoner idag, då de i många fall har stora minneskort och lagrar mycket information. Anställda har sin e-post i sin mobiltelefon och annan typ av information som kan vara en säkerhetsrisk om den kommer i fel händer. Han berättade om att i Windows Mobile har man en funktion för att låsa telefonen om man inte använder den på några minuter, man måste sedan skriva in sitt lösenord för att den ska låsas upp. Skulle man bli av med mobilen var det en bra lösning att använda en teknik som kallas för ”remote wipe”, man skickar ett ”poison pill” till sin mobiltelefon vilket gör att all information raderas och den går tillbaks till det läge den hade när man köpte den. Skyddet på mobiltelefoner är idag nästan obefintligt och det är en skrämmande utveckling.

Per förstärkte BITS tes om att stöldproblemantiken när det gäller mobila enheter skall beaktas. Stöldbenärligheten är enorm på just sådana produkter det händer väldigt lätt att man lämnar enheten oskyddad för en kort stund och då passar tjuven på.

> ”Man står på krogen och lägger upp mobiltelefonen på disken eller på bordet och så står man och dricker en bärs o vänder ryggen till och sen när man vänder sig tillbaka så är mobiltelefonen borta.”, Per Hellqvist, Symantec

Att samma säkerhet som gäller på jobbet skall gälla även när man tar ut enheter från arbetsplatsen är något som Per sammanfattade i en tumregel.

> ”Vem får har vilken information på vilken enhet?”, Per Hellqvist, Symantec

Där man då i första hand tänker på är vem personen är, vad är hans yrkesroll och vilken information har han tillträde till i sin yrkesroll? Nästa steg är att se vilken information den anställda vill hantera. Är den öppen, hemlig eller intern? Sedan skall man se vilken typ av enhet personen vill hantera informationen på och vad det finns för alternativ när det kommer till att skydda enheten. Det är först då man har besvara dessa frågeställningar som man kan ta ställning till om samma säkerhetsnivå kan gälla på den mobila enheten som den på övrig hårdvara i organisationen menade Per.

4.6 Styrning av kommunikation och drift

4.6.1 Driftrutiner och driftansvar

Säkerhetsinstruktioner för säkerhetskopiering, återstarts- och återställningsrutiner samt hantering av revisorer och logginformation krävs för att uppnå basnivå enligt BITS. Idag finns inget bra system att på ett automatiskt sätt avgöra vilken information som skall ha vilken klassning, enligt Per. Detta leder till att de anställda tvingas ta ställning hela tiden till hur informationen ska klassificeras, då räcker det att man gör en miss för att det skall bli fel i kedjan. Utan klara säkerhetsinstruktioner för drift tvingas organisationer ta backup på allting och det är i slutänden kostsamt. Något som dock inte företagsledningar bryr sig om berättade Per.

4.6.2 Skydd mot skadlig och mobil kod

Per menade på att flera företag slarvar eller medvetet låter bli att inte uppdatera eventuella uppdateringar för program. Det fanns flera anledningar varför inte vissa företag gör det.

Ett av dem är att företagen är rädda att nya problem kommer att dyka upp i och med den nya uppdateringen eller så anser de att den äldre versionen av programmet fungerar så pass bra att det inte behövs. En annan anledning är den ekonomiska aspekten, ju större företag man har desto dyrare blir det att göra de här utrullningarna av patchar i organisationen. Per gav ett exempel på att det kostar Skanska en miljon kronor för att skicka ut uppdateringar till alla datorer på företaget. Många av systemen som man måste uppdatera kan heller inte tas ur bruk eftersom man måste vara online hela tiden. Även outsourcing nämndes som ett alternativ till varför man inte var helt uppdaterad. I vissa fall sitter man fast i outsourcingavtal med andra företag vars uppgift är att uppdatera företagets klienter. Är det då någon brist i kommunikationen eller annat så kan det vara så att man inte ens kan uppdatera sin programvara för att man i princip inte äger sina maskiner utan det är outsourcingpartnern som skall göra det åt en. Däremot nämnde han att nackdelen med att sitta fast i äldre versioner är att nya versioner kanske innehåller bättre säkerhet än vad som fanns i dem gamla även fast man har patchat dem och säkrat upp dem till fullo. Så man skall avgöra behoven från fall till fall. Med sådana enorma kostnader det är för flera företag så är det viktigt att testa uppdateringarna och patchar ordentligt, utvärdera dem och se hur de kommer att ändra nätverket.

Johan berättade att tankarna om patchhantering blev aktuellt runt år 2003, då flera nätverksmaskar slog till. Enligt honom hade företagen blivit ganska bra på att uppdatera operativsystemen och Officepaketet, men släpade efter när det gällde annan mjukvara. På PDA och mobiltelefoner är patchhantering nästan obefintlig. Det primära var enligt Johan att se till att företagets datorer alltid hade de senaste uppdateringarna för operativsystem och webbläsare.

Magnus ansåg att man skulle skilja på uppdatering och säkerhetsuppdatering. Han nämnde även att till exempel Microsoft har klassificerat sina säkerhetsuppdateringar i fyra olika kategorier, låg prioritet, medium prioritet, viktig och kritisk berättade han. På så sätt uppfattar kanske användarna det som mer akut när en högprioriterad uppdatering kommer, speciellt bland småföretag som kanske inte har en egen IT-ansvarig menade han.

Samtliga informanter nämnde vid flera tillfällen att det är viktigt att ha uppdaterad programvara, framförallt antivirusprogram och operativsystem. För basnivå krävs det att företaget har rutiner för patchhantering av operativsystem och applikationsprogram, det vill säga övriga programvaror som användarna har till sitt förfogande.

> ”Det är då det primära, se till att man har en patchmanagementstrategi för företaget,” Magnus Lindkvist, Microsoft

Enligt Per så är ett stort problem för organisationer är att hinna uppdatera sig om vilka nya sårbarheter som dyker upp, vad de innebär och vad man kan göra åt dem. Han nämnde att det dyker upp i snitt upp ungefär 10 nya sårbarheter om dagen om man räknar in alla operativsystem och applikationer som finns. Om man håller sig uppdaterad med patchar så är det relativt få av dessa sårbarheter som drabbar datorn, men Per ansåg att det i verkligenheten tyvärr inte såg ut så.

Ett problem som enligt Per flera företag har är att kontrollera att en ny patch eller uppdatering är installerad på samtliga klienter ute i nätverket. Anställda kan vara på semester, pappalediga eller liknande och då kan det hända att deras datorer inte är tillängliga när en ny uppdatering rullas ut.

Så fram till dess att man har det bekräftat att varje dator har fått patchen eller uppdateringen installerad och verifierad att den är installerad och klar, så måste man anse att nätverket inte är helt säkert förklarade Per. Med i genomsnitt tio nya sårbarhetslarm plus uppdateringar till dessa som kommer varje dag, så hinner man inte ofta inte patcha mot allting, man tvingas att välja och det gäller att då veta vilka sårbarheter man skall reagera först och snabbast mot. Det betyder att patchhanteringen måste fungera och ligga i bakgrunden och arbeta. Per nämner även att man samtidigt inte kan förlita sig på det som skyddsmekanism utan att det måste finnas där som ett skyddsnät.

BITS menar att användarens rätt till att installera program eller andra administrativa uppgifter skall regleras och dokumenteras i en säkerhetsinstruktion. Magnus såg på det här med identiteter mer som en trend, förr i tiden hade man inte så mycket identiteter som man har idag och det är en problematik som en modern IT-chef får brottas med, något som dock är en bra lösning enligt Magnus. Det som de flesta tittar på idag är hur man kan se till att användarna har de minsta möjliga rättigheterna som de behöver för att utföra sina arbetsuppgifter, istället för tvärt om. Magnus nämnde ett system som gick ut på att man måste be om rättigheter för att komma åt den önskade informationen eller platsen och då har man på så sätt implementerat ytterligare ett lager av säkerhet i sin arkitektur.

Att begränsa användarnas möjligheter till att begå misstag är något som även Per ansåg som väldigt bra. Helst skulle inte ens datoradministratörer ha administrativa rättigheter längre än vad som krävs. Per nämnde också att någonstans mellan 70-80% av alla incidenter på företag är orsakade av felaktiga konfigurationer eller att man har fel rättigheter och liknande saker, vilket styrker problemantiken inom detta område idag.

Hur viktigt det än är med säkerhet så menade Per och Magnus att det blir som det blir i ute verkligheten. Folk är vana att använda sina datorer som deras egna, man vill personifiera dem även på jobbet. Med begränsade rättigheter blir detta svårt eftersom man inte ens kan ställa in klockan om man inte är lokal administratör. Även IT-personalens resurser sätts på prov eftersom de får väldigt många förfrågningar hela tiden på grund av att de är dem enda som kan ändra inställningar eller installera program på datorerna. Man skall generellt sätt inte ha fler rättigheter än vad man absolut behöver i sin yrkesroll.

> ”Det är därför det heter administrativa rättigheter för att administratören skall ha dem, när han gör administrativa saker.” Per Hellqvist, Symantec

När det kommer till BITS riktlinjer om att skydda sig mot skadlig kod låg finns det inte något optimalt sätt att uppnå detta berättade Per. Man kan däremot begränsa möjligheterna att infekteras och skadverkningar av en eventuell infektion. Enligt Per nådde man det genom att ha så kallad lager-på-lagersäkerhet, samt att arbeta med kraftfulla verktyg för backup och återställning av system.

En annan möjlighet var enligt Per att dela upp organisationens nätverk i mindre enheter med hjälp av segmentering, detta för att se till att en infektion endast drabbar en mindre del av nätverket, något som Johan nämnde som ett bra sätt att minska spridningen av ett utbrott orsakad av skadlig kod. BITS nämner segmentering som en fråga att beakta. Per la fram att segmentering har fallit lite i glömska de senaste åren men att det är ett utmärkt sätt för att få möjlighet att stänga av delar av nätverket. Detta för att rensa upp och begränsa spridningen av elak kod som han utryckte det. En annan punkt som alla tre informanter nämnde som extra skydd och med ett lager-på-lager-förhållningssätt, är att det ska finnas personliga brandväggar på enskilda datorer för att internt i nätverket skydda dem från varandra, samt att skydda dem från

hot när de är utanför företaget. Detta är något som inte nämns i BITS. Även Johan var av åsikten att en bärbar dator ska ha en personlig brandvägg, även vid distansarbete från en personlig dator i hemmet ska det finnas brandvägg enligt informanterna. Johan menade att det fanns en stor risk att skadlig kod såsom trojaner och maskar kom in i företagets nätverk när en anställd arbetade med sin bärbara dator utanför företaget, om den bärbara datorn inte hade ett lager-på-lager-skydd.

4.6.3 Säkerhetskopiering

Säkerhetskopiering skall enligt BITS genomföras regelbundet och det är systemägarnas ansvar att besluta om tidpunkten för detta. Men även vad som skall sparas och var. Per ansåg att det är bra att kombinera inkrementella backuper mellan de stora fulldiskbackuperna, för att efteråt flytta dem vidare till billigare backuplösnigar såsom tejper eller andra lagringsformat, som man sedan flyttar ut från företaget. Eftersom de backuper man skapar även måste finnas på andra platser ifall det värsta skulle hända, exempelvis brand. Detta var även något som Magnus nämnde tillsammans med att man även gärna skulle kryptera informationen innan man skeppar iväg den, om informationens klassificering krävde det. Johan berättade att just säkerhetskopiering var något som han tyckte att företag slarvade med. Företag säkerhetskopierar ofta informationen på filservrar etcetera ,men inte så mycket av informationen på mobila enheter. Framför allt inte på handdatorer menade han.

Även vid mobila enheter saknas det goda rutiner för backuper enligt Per, eftersom vid scenarios som innehåller borttappade enheter kommer det att ta väldigt lång tid att återställa informationen på datorn så den anställda snabbt kan börja komma igång igen. Även om man har gjort en backup så vet man oftast vilken information som försvann med enheten. Backuper kan alltså förhindra att man slipper spendera resurser på att leta reda på och återskapa data.

Även klassificering spelar stor roll när det gäller backuper, enligt Per, ett problem man kan få när man inte har klassificerat sin information ordentligt är att man inte vet vad man måste ta backup på, eftersom man inte vet vilka maskiner som håller riktigt känslig data måste man ta backup på allting. Då finns det risk för att det blir en onödigt stor backup eftersom man råkar få med Mp3-filer och semesterbilder etcetera berättade han.

4.6.4 Hantering av media

BITS anser att klassificering av information är metoden för att kunna avgöra vilka datamedia som skall skyddas mot obehörig åtkomst. Är datamedian öppen information så krävs det inte så pass många nivåer med säkerhet. Men om det är intern eller hemlig information så får man tänka på att lägga några extra lager med säkerhet och kanske till och med ta en extra tankeställare om man verkligen skall ta med sig den här informationen utanför organisationens ”väggar”. Både Magnus och Per nämnde vid upprepade tillfällen att klassificeringen av information är en väldigt viktig del av informationshanteringen.

4.6.5 Utbyte av information

Även med det bästa antivirusskyddet och den största brandväggen räcker det med att en enskild användare gör ett misstag för att hela säkerhetskedjan riskeras att brytas enligt Magnus. Men genom konstant utbildning kring regler för hantering av e-post och att ha tydliga riktlinjer för

klassificeringen av informationen kan man öka säkerhetsmedvetandet hos de anställda. Även rapporteringen från användarna är en kritisk del i incidentrapporteringsprocessen.

4.7 Styrning av åtkomst

4.7.1 Verksamhetskrav på styrning av åtkomst

Inom BITS kategorin Verksamhetskrav på styrning av åtkomst påpekade Magnus och Per att om möjligt ska användarna endast få tillgång till de system som de behöver för att utföra sina arbetsuppgifter. Möjligheten till loggning av händelser i informationssystem gav enligt Per också en liten möjlighet för att spåra vart information har tagit vägen och vem som har gjort vad med den.

4.7.2 Styrning av användares åtkomst

När det gäller Styrning av användares åtkomst var informanterna av åsikten att användaren ska se till att han låser sin arbetsstation och loggar ut för att förhindra obehörig åtkomst. Det var enligt Johan på användarens ansvar att se till att man låser sin dator när man lämnar den, om än för en kort stund. Magnus menade att det var en bra lösning att inte låta användare få installera program, Per höll också med om detta och påpekade att det är bara administratörer som ska få installera program, vilket även poängteras som ett krav i BITS. Magnus och Johan berättade att man kunde ha en policy för skärmsläckare som automatiskt slogs på om man lämnade datorn, för att logga in igen får användaren skriva in sitt lösenord. Något som även är ett krav för basnivå. Annars kunde vem som helst sätta sig ner vid en dator som för stunden är obevakad, läsa e-post och komma åt information och informationssystem som denne annars inte skulle ha tillgång till.

Magnus berättade om att ett ännu bättre lösning var att använda smarta kort för att logga in på sin dator, och samma kort kanske används för att passera ut och in i lokaler inom företaget. Då kan datorn automatiskt låsas när man går ifrån datorn för att ta sig någon annanstans i företaget, givetvis har kortet även en PIN-kod berättade han. Per påpekade också att man ska se till att inte lämna dokument med känslig information på sitt arbetsbord, man bör också ställa undan lösa backupenheter, cd-skivor och annan lagringsmedia, och inte ha det framme på sitt arbetsbord.

4.7.3 Användares ansvar

När det gäller lösenord var Magnus av meningen att man måste använda något som kallas för starka lösenord. Ett starkt lösenord består av åtta tecken, minst en stor bokstav, minst en liten bokstav och minst ett alfanumeriskt tecken. Med dagens datorkraft tar det ungefär 14 miljoner år att knäcka ett starkt lösenord enligt honom. Han menade också att man gärna kan ta ett längre lösenord, en tips från honom var att ta en mening man lätt kommer ihåg, byt ut några tecken mot kraven för ett starkt lösenord så har man ett otroligt starkt lösenord. Det var av vikt att ledningen styrde och kontrollerade dessa lösenordskrav med jämna mellanrum. Per och Johan ansåg också att ett så kallat starkt lösenord var ett krav. Vidare höll Per med BITS rekommendationer om krav på byte av lösenord, och att man ej ska kunna återanvända gamla lösenord, men det fick inte gå till överdrift, byte var tredje månad hade han som riktlinje om man då inte misstänkte att någon annan hade fått reda på lösenordet.

Precis som BITS var informanterna av åsikten att det var organisationens skyldighet att informera användarna om de instruktioner och regler som de är i behov av för att utföra sina arbetsuppgifter. Likväl menade Per och Magnus att det var organisationens skyldighet att ha tydligt uppsatta rutiner för hur man ska hantera användares behörighet när de slutar eller byter arbetsuppgifter, vilket även är ett krav för basnivå.

Enligt BITS målformulering för användares ansvar ska de förhindra obehörig åtkomst och stöld av information och informationsbehandlingsresurser. Per menade att för att uppnå detta krävs det att användaren går igenom tre steg. Användaren ska läsa policys och instruktioner, förstå innebörden av dessa och sist utföra det som står i policys och instruktioner. När man detta är chansen stor att användaren lyckas med ett bra informationssäkerhetstänk menade Per. Magnus var också inne på den linjen, han menade att det är användarens ansvar att följa uppsatta policys etcetera, men i slutändan är det ändå ledningens ansvar att försäkra sig om detta skett som vi även nämnde tidigare. Magnus menade att det också är varje anställds ansvar att vara misstänksam och uppmärksam på människor som kanske befinner sig på ett ställe där de inte ska vara, för att exempelvis förhindra och upptäcka obehörig fysisk access till en dator.

4.7.4 Åtkomst till nätverk

BITS kategorin styrning av åtkomst till nätverk beskriver att om trådlösa nätverk används är det ansvarig för nätverket som ska besluta om åtgärder för att förhindra obehörig avlyssning och nyttjande. Magnus och Per påpekade precis som BITS att WEP-kryptering inte var tillräckligt. Per beskrev det på följande sätt, att har man trådlöst nät har man det ofta för att just få möjlighet till mobilitet, vilket även Magnus vidhöll. Per beskrev det som att om man inte kör med exempelvis en VPN ska man anta att informationen kan spelas in och avlyssnas. Det finns även andra hot mot trådlösa nätverk, Per berättade att man kan modifiera en babymonitor och använda den för att störa ytterfrekvensbandet, och på det viset få ett helt företags nätverk att gå ner.

Johan var av uppfattningen att företag var väl medvetna om problematiken kopplad till trådlösa nätverk, men det var värre hos hemanvändarna, vilket kan ställa till problem vid distansarbete då hemmanätverket använder sig av trådlöst nätverk. Ett annat problem som Johan informerade oss om var att anställda ibland installerar egna trådlösa accesspunkter inne i företagets nätverk, för att förenkla för dem själva. Exempelvis för att få möjlighet att arbeta från konferensrum etcetera. Problemen som uppstår då är att de ofta blir felaktigt konfigurerade, vilket medför ett hot mot informationssäkerheten menade han.

> ”Det är ett jätteproblem, jag vet många företag där en anställd har tagit med en basstation och sedan stoppat in den i företagets nätverk.” Johan Jarl, F-Secure

När det gällde trådlösa nätverk ansåg Magnus att man idag kan bygga säkrare nätverk med trådlös teknik än med ett traditionella nätverk (trådade). Detta för att man då relativt enkelt får en möjlighet att kontrollera alla nya enheter som ansluter till nätverket, han berättar om att när man kör ett traditionellt nätverk kan någon smyga in en dator eller trådlös accesspunkt och koppla in den i ett obevakat nätverksuttag, det är inte alltid man har något skydd när det gäller nya enheter som ansluter till nätverket berättade han, utan oftast får enheterna en IP-adress automatiskt när de ber om det. Vidare lade Magnus fram att en bra lösning för ett säkert trådlöst nätverk exempelvis var byggt på en PKI-infrastruktur (Public Key Infrastructure). Det innebär att man får ett normalt sätt oskyddat nätverk att bli säkert med hjälp av ett kryptonyckelpar, en publik och en privat nyckel. PKI bygger på asymmetrisk kryptering. Han förespråkade en lösning som

byggde på ett användarcertifikat och ett maskincertifikat, för att på det viset försäkra sig om att både hårdvara och användare är den de utger sig för att vara. De både certifikaten står i beroende av varandra och kan inte användas enskilt eller i kombination med andra människors eller maskiners certifikat.

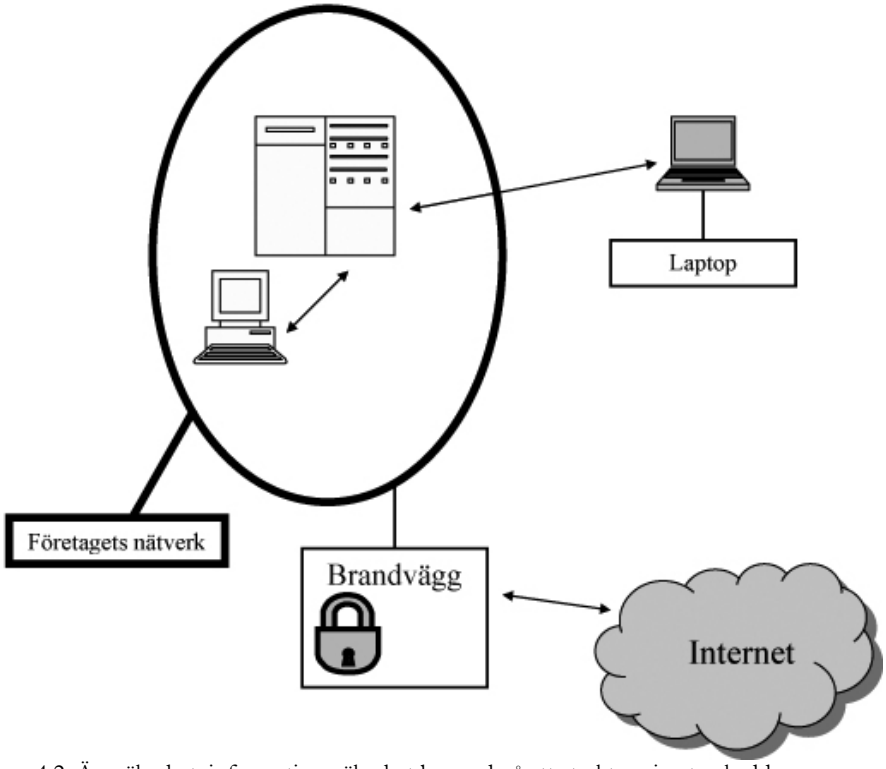
> ”Har man inte rätt maskincertifikat eller användarcertifikat kommer man inte in, och de två måste vara rätt kombination. Jag kan inte ta mitt maskincertifikat och lägga det på en annan dator, eller ta mitt användarcertifikat och logga in med det på en annan dator. Utan de två måste stämma överens om jag vill komma åt nätverket, stämmer de överens har jag den säkra trådlösa accessen.” Magnus Lindkvist, Microsoft AB

4.7.5 Mobil datoranvändning och distansarbete

Om en anställd har en mobil enhet är det hans skyldighet att se till att viktig information på den säkerhetskopieras enligt Per, något som BITS kategorin styrning av åtkomst till information och tillämpningar även har som krav för basnivå. Magnus förklarade att för att lyckas med informationssäkerhet, framförallt när man använder mobila enheter, distansarbete etcetera måste man arbeta med något han kallar för defense in depth, det vi tidigare i denna uppsats nämnt som lager-på-lager-metoden.

> ”Det är lite som allt säkerhetstänk, det finns ingen silverkula för säkerhet utan oftast måste man lösa det här i flera steg, vi kallar det här ”defense in depth.” Magnus Lindkvist, Microsoft AB

Vilket innebär att man ska ha skydd i flera lager, har du en bärbar dator måste den ha en brandvägg, antivirus program. Det måste även ses till att dessa är uppdaterade, men det är enligt Magnus lika viktigt att ha de senaste säkerhetsuppdateringarna till operativsystemet. Tas den sedan in i företagets nätverk ska nätverket ha någon form av karantän funktionalitet. Denna funktionalitet undersöker om datorn har de senast säkerhetsuppdateringarna, om inte släpps den inte in på nätverket. För basnivå krävs inte att man har funktionalitet för karantän, utan det nämns bara att det kan finnas behov av det. Sedan kanske det också finns ett Network Intrusion Detection System (NIDS) som undersöker aktiviteten i nätverket i jakt på onormala aktiviteter orsakade av exempelvis maskar och trojaner påpekade Magnus. Johan var också av åsikten att uppdatering av mjukvara och lager-på-lagersäkerhet på bärbara enheter var av central betydelse för informationssäkerheten, framför allt vid distansarbete. Speciellt poängterade han vikten av att ha operativsystem och webbläsare uppdaterade, då mycket skadlig kod som sprids får möjlighet att ta sig in i datorn just via kända buggar operativsystem och webbläsare.

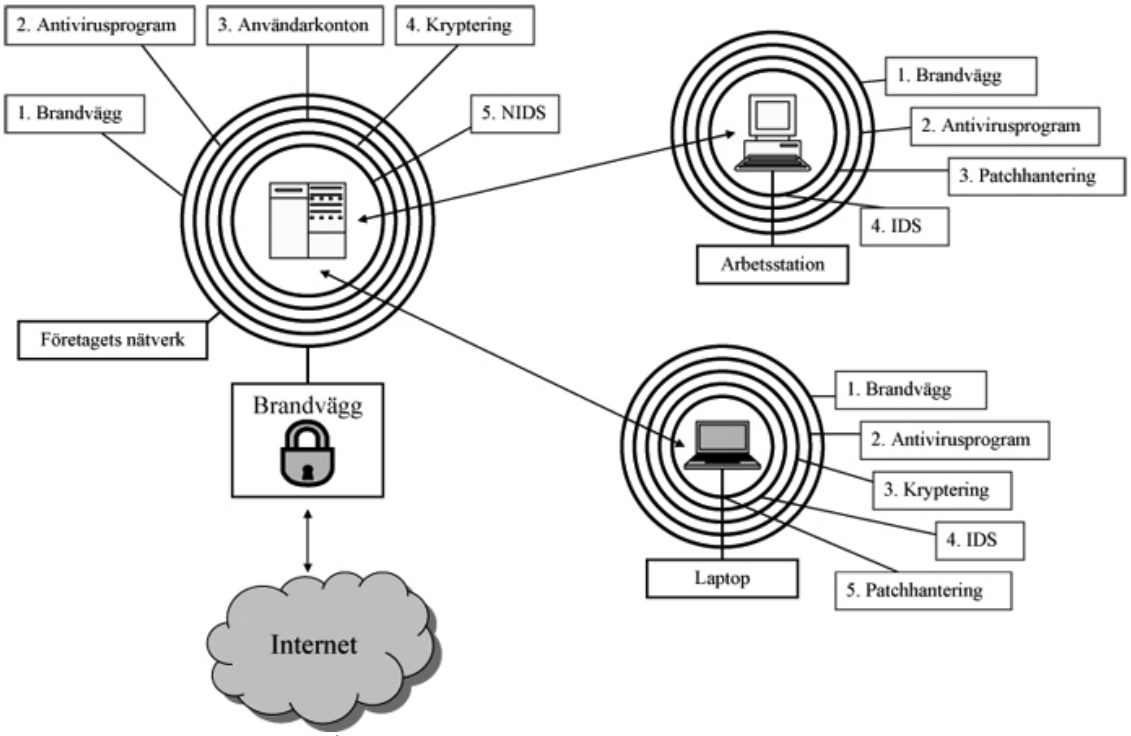


Figur 4.2. Äggsäkerhet, informationssäkerhet baserad på ett starkt perimeterskydd.

Per beskrev samma tänk med orden äggsäkerhet och löksäkerhet. Med äggsäkerhet har man ett perimeterskydd med en brandvägg och ett antivirusprogram med gateway och skyddar företagets nät mot intrång utifrån. Enligt Per är det ett problem att många företag har byggt sin säkerhet baserad på äggsäkerhet med ett starkt perimeterskydd. När användare sedan nyttjar bärbara enheter, och tar in och ut dessa från företagets nät har man där ett stort problem menade Per. Det räcker med att ett e-postmeddelande med en farlig bifogad fil kommer in i nätverket för att allting inom företaget riskeras att smittas, väl inne i nätverket är allting mjukt och mysigt precis som när man knäcker ett ägg utryckte han sig. Motsatsen till äggsäkerhet, löksäkerhet är det Magnus kallade defense in depth.

> ”Om man har löksäkerhet har man lager på lager med säkerhet utanpå varandra som för att säkra kärnan täcker upp och skyddar.” Per Hellquist, Symantec

Med lager-på-lagersäkerhet spelar det enligt Per ingen roll om något farligt kommer genom perimeterskyddet, tar man exempelvis ut sin dator från företaget bär man med sig säkerhet. På sin bärbara dator ska man ha antivirusprogram, brandvägg och möjligtvis ett Intrusion Detection System som övervakar nätverkstrafiken, givetvis måste man se till att ha de senaste uppdateringarna även för operativsystemet enligt Per.



Figur 4.3. Lager-på-lagersäkerhet / Löksäkerhet.

Han menade också att kryptering av information på mobila enheter är ett måste om dessa enheter lagrar viktig information, han ansåg även att kryptering måste finnas på minneskort och dylikt som innehåller känslig information. Enligt honom var det inte heller vanligt att folk krypterar informationen på sina mobila enheter, på mobiltelefoner är det nästan obefintligt. Något som även Johan la fram, han menade att kryptering på PDA och mobiltelefoner nästintill var obefintlig, förutom hos några stora företag, företag som hade en väl utvecklad säkerhetsstrategi för mobilitet.

Säkerhetsriskerna ligger bland annat i att mobila enheter är lätta att bli av med, stöldbegärligheten på mobila enheter är enorm som Per utryckte sig. Med mobiltelefoner har du oftast inte ens någon inloggning, vilket i alla fall ger ett litet skydd av informationen. Magnus menade att ett av problemen idag är att man i bärbara enheter kan bära med sig väldigt mycket information, man måste tänka på hur informationen inte ska kunna komma i fel händer, och vad som kan hända om jag skulle bli av med den aktuella informationen. Enligt Magnus måste man klassificera informationen och skydda den med kryptering om det är känslig information. BITS behandlar inte kryptering på mobila enheter annat än att kortfattat nämna att det kan tänkas behövas ha i åtanke vid användning av mobila enheter. Vilket står i rak motsats till vad våra informanter belyser är av vikt, att kryptering av känslig information på mobila enheter måste genomföras. Avsnittet om kryptering i BITS tar upp att det ska användas vid extern uppkoppling och information ska krypteras om genomförda riskanalyser visar på det.

Att just bestämma hur informationen på mobila enheter ska skyddas verkar återigen vara ett problem, BITS påpekar att det är upp till systemägaren att bestämma hur hanteringen av mobila enheter ska skötas och dokumenteras i säkerhetsinstruktionen för användarna, vilket även våra informanter påpekade. Ett annat problem som våra informanter la fram var att det är återigen en fråga om klassificering av informationen som ska avgöra hur enheten ska skyddas, ett annat

problem som tidigare nämnts är att veta var informationen finns, på vilket enhet. Vilket även belyses av Per. Han menar att för att veta hur man ska skydda sina mobila enheter ska man återigen gå igenom frågan vem får ha vilken information och på vilken enhet. Om man tänker igenom denna fråga varje gång en anställd kommer och vill göra någonting kommer man väldigt långt enligt Per.

När det gäller distansarbete så var det enligt våra informanter absolut viktigast att ha en lager-på-lagersäkerhet, samt att köra säkra uppkopplingar mot företagets nätverk, exempelvis via VPN. BITS poängterar att VPN kan användas om säkerhetsbehovet finns men nämner ingenting om att förbereda den mobila enheten för andra miljöer än företagets egna nätverk, vilket som tidigare nämnts poängteras om och om igen av våra informanter.

4.8 Anskaffning, utveckling och underhåll av informationssystem

4.8.1 Kryptering

Som tidigare nämnts ansåg våra informanter att kryptering måste användas så fort information lämnar företaget, och då om informationen hamnar i fel händer och om informationen då skulle kunna orsaka organisationen skador BITS nämner endast att kryptering kan komma att behövas men är definitivt inte lika propagerande för kryptering som våra informanter.

4.9 Hantering av informationssäkerhetsincidenter

4.9.1 Rapportering av säkerhetshändelser och svagheter

Enligt BITS så krävs det fastlagda rutiner för hur användare skall agera vid misstanke, funktionsfel samt andra störningar. Per talade om ett fall där en IT-säkerhetschef fick en anställd avskedad för att personen hade klickat på en fil bifogad i ett e-postmeddelande och på så sätt råkat infektera företaget med virus. Personen hade sedan anmält detta för IT-ansvariga och sedan blivit avskedad för detta. Per tyckte detta var idiotiskt gjort att bestraffa den anställda genom att avskeda honom. Det som händer då är att ingen någonsin kommer att erkänna någonting hädanefter. Då händer det lätt att IT-avdelningen inte vet vad som händer ute i organisationen. Han punkterade tydligt vikten av att skapa en atmosfär som uppmuntrar till att folk rapporterar märkliga saker. Framförallt är det supportavdelningen eller IT-avdelningen som absolut måste ha öronen öppna för förfrågningar om märkligheter i nätverket. Även när en anställd har rapporterat in någonting så är det viktigt för miljön på företaget att personen kanske får en klapp på axeln, som tack för hjälpen, istället för en bestraffning eller liknande. Får man ut en sådan stämning och klimat på företaget så uppmuntrar man den här typen av beteende, för det värsta som kan hända är att man straffas för ett oriktigt beteende fast man egentligen ville väl, eller man gjorde någonting av misstag, eller man gick på en luring som var väldigt snyggt uppsatt. För om man börjar med hårdare bestraffningar förhindrar man att konstigheter upptäckts vilket i sin tur kan skada företaget mer i längden.

Magnus pratade om ett system för rapporteringar av misstänkta händelser någonting som kallas ”whistle blower” som flera företag har implementerat idag. Funktionen går ut på att en anställd på ett företag kan ringa, e-posta eller faxa in anonymt och säga det, att här är något som försiggår

som jag inte tycker stämmer överens med de etiska regler eller lagar som vi har här på organisationen. Informationen från våra informanter stärker det som BITS specificerar inom kategorin hantering av informationssäkerhetsincidenter.

4.9.2 Hantering av informationssäkerhetsincidenter och förbättringar

Per menade att organisationen snabbt och effektivt måste reagera på incidentrapporter. Direkt efter en händelse ska man sätta sig ner och titta igenom vad som har hänt, varför det har hänt och hur man kan förhindra att det händer igen. Svaren från informanterna stämmer väl överens med det som framhävs i BITS.

> ”Här gäller det att på ett öppet och ödmjukt sätt erkänna att något gått fel och ha viljan att rätta till det så att det inte händer igen. Lär man sig inte när något gått fel har man gjort ytterligare ett fel.” Per Hellqvist, Symantec AB

5 Slutsats

Det råder inga tvivel om att det finns väldigt mycket att göra på informationssäkerhetsområdet när det kommer till problematik kopplad till användandet av mobila enheter. Vår undersökning indikerar att det nästan är en alarmerande situation ute hos företaget och dessa organisationer har en stor utmaning i att få till stånd en hållbar informationssäkerhetsnivå för sina mobila enheter.

Har då informationssäkerhetssituationen förändrats i takt med det ökande användandet av mobila enheter? Tidigare kunde företagen ofta förlita sig på att de själva hade kontroll över den miljö dess hårdvara befann sig i, när Internet började användas fick man ny problematik, med att skydda sitt nätverk från attacker utifrån. Nu måste de även skydda sina nätverk inifrån, i och med att enheterna tas ut ur företagets nätverk, för att sedan tas in igen. Undersökningen visar även på att med mobilitet kommer nya problem med nätverksarkitekturen. Trådlösa nätverk är tätt sammankopplade med mobilitet och företag verkar inte riktigt veta hur de ska skydda sina trådlösa nätverk ur ett tillfredställande informationssäkerhetsperspektiv.

Ett annat resultat av undersökningen är att det övergripande problemet med informationssäkerhet och mobila enheter är att företag ofta har ett bra perimeterskydd, men allt för sällan lager-på-lagersäkerhet som våra informanter påpekade. Andra till synes stora problem är att informationen på mobila enheter väldigt sällan är krypterad, och det blir en säkerhetsrisk i och med att de är stöldbegärliga. Detta tillsammans med att företag får svårt att hålla reda på var informationen befinner sig skapar stora problem för informationssäkerhetsansvariga.

BITS är i vårt tycke ett mycket bra initiativ av Krisberedskapsmyndigheten, men resultaten av vår undersökning visar på att det finns uppenbara brister när det kommer till mobila enheter, och till det tätt sammankopplade trender och tekniker som exempelvis distansarbete. Vi är efter undersökningen av åsikten att BITS hanterar problem med trådlösa nätverk på ett bra och informerande sätt, men brister när det kommer till informationssäkerhet på mobila enheter.

BITS ska endast vara minsta acceptabla nivå för informationssäkerhet, men vi anser ändå att det måste tillföras mer riktlinjer för mobila enheter. Detta eftersom mobila enheter och mobilitet inte kommer att försvinna, snarare tvärtom. Vid användandet av mobila enheter ska enligt vår åsikt lager-på-lagersäkerhet implementeras, något som även stöds av Hietala (2004) och Straub (2003). Via vår undersökning har vi fått uppfattningen att det är ett absolut måste, dels för att skydda enheten när den är i andra nät än företagets egna, men även för att skydda enheten i företagets interna nätverk. Eftersom det inte är ett krav för basnivå att enheter som förs in i nätverket igen går igenom någon form av karantän funktionalitet är lager-på-lagersäkerhet med uppdaterad brandvägg, antivirus, operativsystem och webbläsare ännu mer ett måste. Detta för att förhindra att företagets nätverk blir infekterat av skadlig kod, eller för med sig andra hot mot informationssäkerheten.

En annan punkt som undersökningen har fått oss att anse är att BITS borde definiera att lösenord ska vara ett så kallat starkt lösenord, vilket inte definieras idag, men poängteras av våra informanter och Boeckeler (2004). BITS är av åsikten att antivirusprogram och operativsystem ska vara uppdaterade, men inte att varje enhet ska ha en personlig brandvägg. Just personlig brandvägg på varje enhet är något som informanterna var väldigt överens om, men även

Rosenberry (2003), Trend Micro (2005) och Hietala (2004) påpekar detta. I dagsläget belyser BITS vikten av att ha rutiner för patchhantering inom organisationen, men de borde poängtera det som är primärt att uppdatera för mobila enheter, operativsystem, antivirusprogram, brandvägg och webbläsare, så att man skyddar enheten när den är utanför företaget då undersökningen har visat att det finns en stor hotbild mot dessa när de lämnar företagets domän.

Ytterliga en punkt som undersökningen visar att BITS borde behandla mer är frågan om att organisationer måste konfirmera att utbildning och säkerhetspolicys har tagits upp av och implementerats korrekt av användarna, vilket även Rosenberry (2003) och Trend Micro (2005) anser. Detta för att organisationerna ska få möjlighet att utvärdera och genomföra förändringar. BITS menar att man ska granska sina policys, men det borde specificeras mer tydligt att det måste försäkras att dessa policys har tagits upp av organisationen.

En annan utbildningsfråga som vår undersökning poängterar är den om att utbilda användarna i informationssäkerhet, få dem att aktivt tänka på hur de arbetar, helt enkelt öka informationssäkerhetsmedvetandet hos organisationens anställda. BITS nämner detta under några kategorier, men det bör enligt oss belysas mer, speciellt vid nyanställningar.

5.1 Förslag på vidare forskning

Som vid flera tillfällen nämnts i denna uppsatts är mobilitet en trend som inte kommer att minska de närmsta åren. Allt mer företag väljer mobila lösningar och fler privatpersoner anammar mobila enheter. Det hade varit intressant att kontinuerligt forska vidare inom detta område för att följa utvecklingen och identifiera eventuella problem som kan uppstå.

Även fältstudier ute i företag skulle bidra med mer information om hur organisationer hanterar problematik kopplat till användandet av mobila enheter. Det skulle vara speciellt intressant att genomföra en studie i organisationer som implementerat BITS och se hur de har konfronterat riskerna och hoten. Experterna som intervjuades i vår undersökning representerade en form av produktsäljande företag, även om de tre företagen också har ett stort tjänsteutbud. Därför skulle det vara av intresse av att undersöka vad säkerhetsföretag som enbart är tjänsteleverantörer har för åsikter om säkerhet kopplat till användandet av mobila enheter.

Bilaga 1, Begrepp

5.2 VPN, Virtual Privat Network

VPN står för Virtual Private Network, vilket möjliggör att segregera trafik från annan trafik och skapa en säker privat förbindelse över ett publikt nätverk, exempelvis Internet. Flertalet organisationer utnyttjar uppbyggda VPN-tunnlar internt och externt genom att för ett speciellt ändamål bygga upp ett gemensamt virtuellt nätverk mellan sig. Ett exempel på varför man bör tillämpa VPN är när någon till exempel är på affärsresa och måste koppla upp sig mot företagets servrar för att arbeta, läsa e-post, hämta filer etcetera. Då kan man utnyttja en VPN-tunnel för att koppla upp sig mot företagets nätverk. Vilket innebär att datorn beter sig som om den skulle vara ansluten på plats i det lokala företagsnätverket (O'Dorisio, 2004) .

5.3 Kryptering

För att säkerställa att data som skickas inte kan läsas av någon annan än personen den är menad för är kryptering en metod för att förhindra just detta. Man brukar tala om två olika typer av kryptering symmetrisk och asymmetrisk kryptering (Stallings, 2003). I symmetrisk kryptering delar man på en hemlig som man använder till att kryptera och kryptera upp data. Det största problemet med dock en symmetrisk nyckel är att säkerställa hanteringen av nyckeldistributionen utan personlig kurir. Vid asymmetrisk kryptering delar man på två nycklar, den publika nyckeln som används för kryptering av data och den privata används för dekrypteringen av data (Stallings, 2003).

5.4 WLAN

WLAN står för Wireless LAN, Wireless Local Area Networks. Det innebär trådlösa nätverk och är ett radiobaserat alternativ till ethernet. Dessa trådlösa nätverk ändvänds mycket ofta i offentliga miljöer så som kaféer, bibliotek, högskolor, flygplatser och hotell. WLAN fick en enorm genomslagskraft 2001 tack vare standarden IEEE 802.11b, som klarar överföring upp till 11 Mbps. Den senaste standarden är IEEE 802.11g, som kom 2003, klara hastigheter ända upp till 54 Mbps och med förbättringar av tekniken har man lyckats komma upp i hela 240 Mbps. Med dessa hastigheter är WLAN ett mycket dugligt alternativ till trådbaserade nät. Eftersom näten är trådlösa så kan vem som helst med ett nätverkskort med support för 802.11 koppla upp sig mot nätverket. Därav måste man ofta reglera eller skydda nätet med olika former av kryptering så som WEP och WPA där WEP är bland det vanligaste man stöter på (O'Dorisio, 2004).

5.5 WEP

WEP står för Wired Equivalent Privacy och är en krypteringsmetod som ingår i standarden IEEE 802.11 för trådlösa nät. Man skapade WEP för att kunna göra de trådlösa näten lika säkra som de trådbundna så man kunde hålla obehöriga borta från sitt nätverk. Det är numera välkänt att WEP inte är något vidare skydd mot intrång (Arbaugh, 2001), det finns ett flertal program som man kan ladda ner gratis på nätet som gör att vem som helst relativt lätt att knäcka WEP-krypteringen. WPA är en vidareutveckling av WEP (O'Dorisio, 2004).

5.6 SSID

SSID är förkortningen för Service Set Identifier vilket är en sträng tilldelat till en accesspunkt, för att trådlösa enheter ska kunna veta vilken accesspunkt de kan ansluta till i ett trådlöst nätverk (O'Dorisio, 2004).

5.7 IDS, Intrusion Detection System

IDS står för Intrusion Detection System, intrångsdetekteringssystem. Ett IDS-system analyserar trafiken i ett nätverk för att sedan identifiera och förhindra intrångsförsök (O'Dorisio, 2004) .

5.8 Skadlig och illvillig kod

Skadlig kod definieras enligt rapporten Beredskap mot skadlig kod (Krisberedskapsmyndigheten, 2005) som program som sprider sig själva och som tränger in i system via olika kanaler. De viktigaste kanalerna är e-post, Internetsidor och smittade lagringsmedia såsom USB-minnen. Skadlig finner man i maskar, trojaner, spyware etcetera. Skadlig kod orsakar just skada på informationssystem som blir smittade, medan illvillig kod inte alltid direkt orsakar skada. Illvillig kod kan ha annat uppsåt än att skada informationssystemen i fråga, som exempelvis samla in uppgifter om informationssystemets användande.

5.9 Phising

Phising är ett försök av en tredjepart att söka efter konfidentiell information från en individ, grupp eller organisation, har ofta sitt ursprung i finansiella syften. ”Phisers” är en grupp människor som lurar andra människor att ge ifrån sig personlig information så som kreditkortsnummer, bankkontonummer och annan känslig information. Phising kan delas upp i två delar: Phising-meddelanden och phising-försök. Ett phisining meddelande är ett unikt meddelande som skickas till en individ med syfte att försöka få tag i konfidentiell eller personlig information från individen. Varje phising-meddelande har olika innehåll för att lura mottagaren att släppa konfidentiell information. Ett phising-försök defineras som en instans av phising-meddelanden som skickas till en enskild användare. Ett försök kan bestå av ett eller flera olika unika phising-meddelanden i ett försök att lura mottagaren (Symantec, 2006).

5.10 Bots

Bots (förkortning av Robots) är program som installeras i hemlighet på datorn. Bots ger möjlighet för någon att fjärrstyra datorn. De är designade för att ge en dataattackerare möjlighet att skapa ett nätverk med ”Bot-infekterade” datorer även kallat Bot Network, vilket kan kontrolleras via fjärrstyrning och kollektivt genomföra aktiviteter som DoS attacker (Symantec, 2006).

Detta kan skapa enorma säkerhetsrisker för företag. En dator som har en bot installerad kan sätta ett helt nätverk i farozonen. Om denna dator kopplas upp mot företagsnätverket så kan boten få fritt spelrum rakt in i företagets nätverk genom den infekterade datorn. Även om dessa datorer har det bästa och senaste skyddet mot olika dataattacker hjälper inte detta eftersom den infekterade datorn oftast anses som en trovärdig klient och på så sätt kan boten söka efter vad som helst inom nätverket, och sedan skicka tillbaka det till botägaren. Som nämnts tidigare kan även botar användas för att skapa DoS attacker mot företagets hemsidor och andra informationssystem, vilket kan få katastrofala effekter framförallt om man sysslar med e-handel. Problemet med botar blir allt mer alarmerande, under andra halvan av 2005 hade de Bot-relaterade dataintrången ökat med 43 % gentemot första halvan av 2005 (Symantec, 2006).

5.11 DoS-attack, Denial of Service attack

En DoS-attack är en överbelastningsattack mot ett datasystem i syfte att se till att inte någon annan får tillgång till systemet. Genom koordinerade attacker mot en webbplats som bombarderas med nätverkstrafik förhindrar den webbplatsen att utnyttjas till dess vanliga funktioner. En annan variant är attacker som utnyttjar säkerhetshål i mjukvara, attacker som får program eller hela system att krascha (O'Dorisio, 2004).

5.12 Maskar

En annan väldigt vanlig illvillig kod är Maskar (Worms). Maskar är självständiga program som självreplikeras och sprider sig från dator till dator över Internet via kända säkerhetshål, utan att behöva hjälp från någon oförsiktig användare. Det vanligaste problemet med maskar är att systemet blir väldigt belastat och i slutändan tenderar datorn helt enkelt att sluta fungera (Symantec, 2006).

5.13 Trojansk häst

En trojansk häst är ett datorprogram som utger sig för att vara till nytta, men som orsakar skada när det fått en användare att installera det. Trojanska hästar brukar installera olika spionprogram eller ”öppna” någon bakdörr i datorn. Men trojanska hästar kan även förstöra eller ändra filer. Samma användarmedvetenhet kan tillämpas mot trojanska hästar som mot datorvirus. Att alltid kolla igenom suspekta filer eller program med ett antivirusprogram innan man installerar det (Symantec, 2006).

5.14 Spyware och Adware

Adware är program som nekar tillgång till information och istället visar reklam inom samma genre. Adware är väldigt lätt att installera av misstag, det ligger ofta gömt med någon form av gratisprogram eller i speciella hemsidor. Adware skapar inte endast problem med reklam på datorn, Adware kan även bli en säkerhetsrisk. Ibland kan dessa program samla information från datorn så som information kopplat till webbläsaren. Denna information kan sedan skickas tillbaka till något företag som betalar pengar för att se vad folk har för vanor för att sedan ”attackera” dem med ännu mer reklam. Denna sändning av information fram o tillbaka tar upp bandbredd och kan därmed minska datorns funktionalitet och tillänglighet (Symantec, 2006).

Spyware är enstaka program som har möjligheten att leta igenom datorsystem eller följa datorvanor och sedan skicka tillbaka denna samlade data till andra datorer. Den information som samlas in kan innehålla information om lösenord, inloggningar, kontonummer etcetera. Informationen kan lagras via att logga vilka knappar på tangentbordet som tryckts in, eller logga eventuella konversationer i olika chatt-program. Även information angående användarens dator, applikationer eller Internetanvändning kan loggas och distribueras vidare. Spyware kan vara mycket farligt, speciellt när det kommer till identitetsstöld och bedrägerier. Men det finns även funktionella användningsområden för Spyware, företagsledare kan ha Spyware installerat på företagets datorer för att se till att de anställda gör det de skall, eller föräldrar som vill se vad deras barn håller på med när de sitter bakom datorn. Precis som med Adware installeras Spyware i smyg och ofta tillsammans med andra program (Symantec, 2006).

5.15 PDA

PDA är förkortning för Personal Digital Assistant, det är små handhållna enheter, en dator som är liten nog att få plats i handen eller i fickan. PDAs användes till en början mest som fickkalendrar men har numera blivit så pass avancerade så de nästan fungerar som fullständiga datorer, de kan lagra stora mängder med information. På senare tid har de även kombinerats med mobiltelefoner och på så sätt skapat så kallade smarta telefoner vilket i princip är en PDA tillsammans med en mobiltelefon, exempel på detta är Blackberrys, Nokia Communicator etcetera (Price, 2003).

Bilaga 2, Expertintervjuer, ämnesområden

Bakgrund
- Informantens bakgrund
- Arbetsuppgifter

Mobilitet
- Har säkerhetsbehoven ökat? Hur?
- Är bekvämlighet ett problem? Enkelt att koppla in exempelvis ett USB-minne
- Stulen/Borttappad mobil hårdvara, hot, skydd?
- Vilka mobila enheter medför mest risker?
- Vad finns det för framtida hot mot mobila enheter?
- Om illvillig kod kommer in innanför perimeterskyddet, hot, skydd?
- Nya trender, WLAN, distansarbete, hot, skydd?
- Företag är rädda för ny teknik som exempelvis IP-telefoni pg. av säkerhetsrisker?

Driftssäkerhet
- Säkerhetskopiering
- Patchhantering, uppdatering av mjukvara
- Hålla upptid på informationssystem, enheter vid utbrott av skadlig kod etcetera

Standarder
- Informantens syn på standarder som ISO17799
- Är standarder lösningen på problematiken?
- BITS, har informanten hört talas om det?
- Informationsklassificering, ett problem?

Personalrelaterade / Användarrelaterade
- Utbildning av personal, kontinuerlig utbildning för informera om informationssäkerhet och öka medvetandet?
- Är människan ett stort problem, hur?
- Accesskontroll för att se till att inte obehöriga nyttjar resurser
- Begränsade rättigheter för minska spridandet av exempelvis Internetrelaterade hot som maskar, trojaner
- Policys för lösenord
- Risker med Internetanvändning? Spridning av illvillig kod etcetera
- Obevakade arbetsstationer, bärbara datorer, PDAs etcetera
- Användarnas eget ansvar?
- Vad slarvar användare med?
- Skydd mot användarrelaterade hot?
- Incidentrapportering
- Omvärldsbevakning

Företagsspecifika frågor

- Alla informanter. Vilka produkter och tjänster får ni mest förfrågningar om från kunder, företag?
- Magnus Lindqvist, Microsoft AB. Er plattform är mest drabbad av alla plattformar när det gäller Internetrelaterade hot, kommentarer?

Avslutande frågor

- Vad är ditt bästa tips till en användare samt en säkerhetsansvarig?
- Har du blivit drabbad av skadlig kod?
- Varför är informationssäkerhet ett komplext problem?

Bilaga 3, Expertintervju, Magnus Lindkvist, Microsoft AB

Samtalet börjar med en kort presentation om hur intervjun kommer att gå till.

Vi tänkte berätta lite om syftet med den här intervjun och uppsatsen vi skriver. Vi försöker undersöka hur mobila enheter och en del nya trender påverkar informationssäkerheten, hur och vad företag kan göra för att skydda sig mot hot. Kan du börja med att berätta om din bakgrund och arbetsuppgifter på Microsoft?
Jag arbetar då som Cheif Secutiry Adviser på Microsoft och min bakgrund på Microsoft är, jag är inne på mitt elfte år just nu började på supportavdelningen 1995, sen har jag jobbat med support på våra olika operativsystem och produkter. Sen gick jag till vår storkundsavdelning efter det och jobbade med teknisk pre-sale. Sedan efter det flyttade jag till USA och jobbade som säkerhetsprogramchef, security program manager, på någonting som heter Microsoft Security Response Center, MSRC. Och där jobbade jag ett år, sen flyttade jag tillbaks till Sverige och jobbade som strategisk säkerhetsrådgivare på vår storkundsavdelning, sen i december har jag jobbat med min nya roll som CSA, Cheif Security Adviser. Det är en strategisk roll på Microsoft som spänner sig över alla avdelningar, storkunder och våran public sector, det är en kort sammanfattning.

Jag tänkte gå igenom lite snabbt vilka områden vi har önskemål om att gå igenom. Det är då mobilitet, nya trender WLAN och distansarbete och IP-telefoni. Vi har lite kopplat till standarder, och en del kopplade till personalrelaterade frågor. Vi har några MS, Microsoft relaterade och lite avslutande och generella frågor. Låter det bra?
Det låter bra, vilken nivå ska det här ligga på, ska det vara en teknisk nivå, eller mer processnivå, vad är målgruppen för den här uppsatsen?

Det ska inte gå ner på teknisk nivå som hur packet hanteras i routrar, inte så tekniskt, målgruppen är människor som är intresserade av informationssäkerhet och har en viss kännedom inom ämnet, så du behöver inte förklara vad illvillig kod är, eller sådana saker utan bara nämna det.
Ok

Så vi kan ju börja och se hur det går
Det finns en sak jag vill ta upp i det här tycker jag, och det är hur man skriver säker kod. För det är något jag definitivt kommer att ta upp i någon av frågorna som kommer då.

Förlåt en gång till
Det som man borde ta med är hur man skriver säker kod

Ok
Det spelar ingen roll med alla tekniker och funktioner som finns, i slutändan spelar det ingen roll vad man gör. Har man inte skrivit bra och säker kod så kommer det inte att fungera ändå.

Vad är dina åsikter om säkerhetsproblematiken, om den har förändrats i och med att det har blivit mer användande av mobil hårdvara, mobiltelefoner, laptops?

Precis, du svarade på en fråga jag hade direkt där. Mobil hårdvara är det i första hand laptops eller är det telefoner för det är ju lite skillnad på den datamängd som man använder och på olika användningsätt, vi kan ju splitta upp det i två delar.

Ok vi kan börja med datorer då så att säga, bärbara.
Laptops, det är ju inte direkt en ny trend. Det är något som har funnits ett tag Det första operativsystem som är direkt anpassat efter bärbara datorer var Windows 95 tack vare plug'n'play. Ett vanligt kännetecken för laptops är att man ändrar konfigurationen, man kanske stoppar i ett nätverkskort, man stoppar in den i en dockningsstation och då ställer man ju det ett krav på operativsystemet att det kan anpassa sig där efter. Det som jag i dagsläget stött på när det gäller säkerhet och mobila plattformar är mer hur säkrar man den data som finns på ett mobilt system. För ett tag sen hade vi ju ganska begränsad mängd information, man kunde lyfta med sig i datorer, men idag så finns ju väldigt stora hårddiskar till mobila datorer. Så att om man idag får tillfälle till det och har rätt access så kan man lyfta med sig extrema mängder data ut från ett företag. Frågan blir ju därför hur ser jag till att datan stannar inom företaget och på rätt ställe samt hur ser jag till att inga obehöriga får tillgång till min data?

Är det den största problematiken du ser med just laptops, att data kan komma i fel händer, när man flyttar ut det.
Idag slår laptops stationära datorer när det gäller vilka datorer köper företag. Det är mer mobila enheter inne i företagen än stationära om vi pratar rena datorer.

Ja ok
Så trenden är ganska klar då, det här medför ju några problem. Antingen väljer man att anamma den mobila plattformen fullt ut som tillexempel Microsoft har gjort, vi har sagt det att vi ska köra trådlösa nätverk och de som behöver då ska givetvis få tillgång till en laptop. Sen den andra problematiken är att om jag har tillgång till känsliga uppgifter hur ser jag till att de uppgifterna stannar hos mig. Vad händer om jag skulle tappa bort min laptop eller få den stulen.

Ok
Så det här är ju frågor som oroar de flesta företag. Det finns lite olika sätt att lösa det här på, men det är lite som allt säkerhetstänk, det finns ingen silverkula för säkerhet utan oftast måste man lösa det här i flera steg, vi kallar det här "defense in depth", lager på lager metoden. Om man börjar längst ner närmast hårddisken är då kryptering en vanlig metod för att skydda data från att komma i fel händer så om jag tappar min dator så spelar det inte så stor roll om någon säljer den på plattan för femtusen spänn, det är tråkigt, min chef blir arg på mig. Men det skulle vara ett större problem om jag hade hela källkoden för nästa operativsystem på min laptop, och de kunde sälja den för x antal miljoner kronor till en konkurrent.

Du menar att klassning av informationen ungefär ska avgöra om man ska ha kryptering, att man ska klassa information, är det så du menar?
Absolut, klassning av information är ett steg av hur informationssäkerhet implementeras idag på företag. För att om jag inte vet hur jag ska klassa min information kan inte bestämma hur jag ska skydda den, det här är ju ett verktyg för att hjälpa till när jag då har klassificerat min data.

Jaha, en annan problematik som vi har funderat över med mobilitet är att man kan ta ut den ur företaget och använda den hemma. Man kanske tar in den i ett nätverk som inte är lika säkert så att säga, eller så kanske någon obehörig använder den
Precis

Vad finns det för problematik där?

Eftersom jag kommer från ett teknikorienterat företag så är min första insikt som tekniker att det här är ett problem som det går att slänga teknik på och då löser det sig. Men som jag kommer komma in på så är det också så att säkerhet kan du inte enbart lösa med teknik, teknik är ett hjälpmedel och en av hörnstenarna i säkerhetstänket. Om det inte finns en policy i företaget, ett tydligt regelverk för vad som gäller kan du göra hur mycket som helst på tekniksidan. Om en person har fått strikta regler för att du inte får lyfta det här datat utanför företaget eller maila det här utanför företaget, du får inte maila det här till din egen hotmail adress eller vad det må vara. Vet de inte om vad som gäller och när datat då väl flyger ut från företaget tappar företaget kontroll på vart det här tar vägen. I vissa fall måste man ju sätta en regel, eller rättare sagt det måste finnas en policy på företaget där man säger.

Hej kära användare, eller kära medarbetare i det här fallet. Välkommen till vårat företag, det här är de regler som gäller. Så får man läsa igenom dem och ta en diskussion med sin chef om du några frågor eller några saker som du funderar över. Det här är våran informationssäkerhetspolicy, är det här intern information på företaget vilket innebär att man inte ska skicka vidare det till någon, det kanske är klassificerad information vilket då innebär att bara ett fåtal ska ha tillgång till det

Ok.
Bryter användarna mot det här kan ju allt från ett samtal med chefen till uppdraget hos arbetsgivaren avslutas, ibland går det ju så långt som polisanmälan.

Kan man med teknikens hjälp förhindra att man skickar information, i och med att alla har Internet överallt, så det finns inget tekniskt hjälpmedel att stödja en sådan policy, utan det ligger då helt på användarens ansvar?
Nej det finns tekniska hjälpmedel, det viktigaste är att säga som jag vill poängtera här är att det inte finns någon enskild teknik eller policy som löser det här utan oftast en kombination för att få bästa resultat – ”defence-in-depth”

Ok
På Microsoft har vi gjort en lösning som hjälper till med det här och det kallas för digital rights management, eller rights management. Vad den lösningen innebär är att vi har möjligheten att sätta rättigheter på alla e-postmeddelande vi skickar, alla office dokument, word, excell, PowerPoint som exempel. Så att jag kan säga så här . Här har jag ett känsligt mail och det här vill jag endast ska gå till våran styrgrupp, arbetsgrupp, eller endast till oss inom projektet som vi håller på med. Vad som händer då är att då går våran mailserver ut till en såkallad rights management server och ber om dom nycklarna hos de personer jag vill skicka mailet till, krypterar det här mailet och sätter mig som ägare på informationen. Vad det här innebär då är att de personer som får det här mailet måste då så fort som de öppnar det här mailet autenticera sig mot right management servern och bekräfta sin identitet. Först då får de tillgång till nyckeln som gör att de kan öppna mailet.

Tänker man då i förlängningen, jag har kanske gjort ett excell ark med budget eller ett worddokument med känslig information om vår nästa produkt eller liknande, då är det så att, även om jag tar det här worddokumentet och lägger på min laptop, mailar till ett annat konto, eller lägger det på min usb-sticka och någon tar den, varje gång någon ska öppna det här dokumentet måste de autenticera sig mot vår right management server, för att kunna ens öppna det här dokumentet, det innebär då att plötsligt följer krypteringen med informationen och inte på själva mediat

Ok

Problemet är idag är att ja vi krypterar kanske alla hårdiskar på våra laptops. Men det hjälper ju väldigt sällan om någon har tagit ut informationen, printat ut den eller mailat den någonstans. Right management är då ett av de här verktygen vi har för att hjälpa företag när att man har en klassificering och hanterar känslig information så kan man få hjälp av den här rights management funktionaliteten, i förlängningen har vi också en produkt som heter Sharepoint portal server så att istället för använda massa fileshares och jobba mot och slänga in filer i så kan man i nästa version av Sharepoint Portal Server som kommer senare i år sätta upp arbetsgrupper, ifall en arbetsgrupp jobbar med ett visst dokument eller PowerPoint fil eller vad de nu må vara, så hanteras den här right management funktionaliteten av portalen och när jag släpper ett dokument i den här portalen blir det automatiskt skyddat, via den här rights management servicen.

Så det är via drag and drop då, som i vanliga sharepoint och automatiskt krypterar då.
Ja.

Märker ni ett tryck från företag, är det ett sug efter liknande produkter?
Ja det märker vi absolut, man tittar ju på flera olika lösningar i flera olika företag för att lösa det här då. Men framför allt måste man kunna följa upp vart informationen finns någonstans. Hur kan jag sätta restriktioner för vem som får till access till vad? Det som vi kanske använder det till är att skicka känslig information till alla anställda, då kan man skicka ett mail som säger:.I morgon kommer vi annonsera det här och information är ju oftast klassad i tre eller fyra kategorier. Man brukar säga att antingen är den hemlig då klassificerad, intern eller publik. Ibland finns det tre och ibland finns det fyra informationsklassificeringar, information vill ju oftast gå från klassificerad till publik, så att enda dan är den kanske klassificerad, ena dagen kanske den är internal only, tredje dagen kanske den är publik. Och då behöver man ju kunna ändra klassificeringen och kanske låsa upp dokumenten eftersom. Det är en fråga som vi ofta får.

Från krisberedskapsmyndigheten har det kommit information om att många företag är rädda för att använda IP-telefoni pågrund av säkerhetsaspekter. Hur tror du säkerhetsaspekter kan hindra företag från att nyttja tekniker?
Jag tror det finns två sätt att se på det här, antingen så ser man möjligheterna med det här eller så ser man begränsningarna. Det här är en bedömning man måste göra från fall till fall, vad är det för någonting jag är ute efter, är det en billig lösning för att kommunicera i mitt företag? Vi på Microsoft har använt IP-telefoni sen jag vet inte när. Vår huvudväxel i Sverige är ihopkopplad med huvudservern i USA så att alla vet vad vi gör, när jag ringer härifrån till USA sker det via IP-telefoni. Sen har vi det vi kallar för instant messeging, så att när som helst på företaget kan jag då sitta och chatta med folk som sitter vart som helst i ett Microsoft företag, besluter jag mig sedan för att nej det här kanske vi ska ta och prata om istället kan jag med ett enkelt klick gå över till just en voice-kommunikation och sitta och diskutera det här. Om man då är rädd för det här, att det ska finnas problem med det har man ju ytterligare möjlighet att lägga på funktioner för kryptering i sin kommunikation, sen som jag sa innan, det beror ju på vilket behov man har och vilka krav på säkerhet man har för den lösningen som man vill ha.

Om vi kollar på exempelvis WLAN och distansarbete som exempel på nya tekniker, så finns det väl troligtvis risker med dem, vad är det för risker och vilka skydd finns det mot det? Distansarbete kanske går ihop med att man ska ha en säker uppkoppling mot jobbet via en VPN eller något sånt där men du kan väl utveckla lite om risker och skydd kopplat till WLAN och distansarbete exempelvis, för det känner vi att vi skulle vilja ha din åsikt om
Absolut, WLAN antar jag du menar trådlöst nätverk då?

Japp

Microsoft har då världens största trådlösa nätverk, och det har vi haft nu i…jag vet inte, fyra år i alla fall, vi bygger våra lösningar på Microsofts egna serverprodukter, jag hävdar idag och har gjort ganska länge nu att i dagsläget kan du bygga ett säkrare trådlöst nätverk än vad du kan göra med ett trådat nätverk.

På vilket sätt då?
Ja precis, för idag om man traskar in på ett företag, eller en reception så finns det oftast ett nätverksuttag någonstans. Och om du då smyger in en dator och kopplar in den, det kan vara en väldigt liten dator, eller det kan till och med vara så fräkt att det är en liten trådlös accesspunkt och om du då bara stoppar in den där i nätverkuttaget har du oftast access till hela företaget och deras resurser. Det är inte alltid man har gjort något skydd när det gäller nya enheter som ansluter till nätverket, så om det kommer en ny enhet och ber om en IP-adress så får de oftast det och väldigt sällan har man segmenterat nätverket så att det här speciella nätverkuttaget eller den här oauthenticerade ipadressen, vad får dom access till i mitt nätverk utan man litar helt enkelt på det fysiska skalskyddet där. Ett trådlöst nätverk å andra sidan så måste man tänka ett steg längre där, man kan ju sitta ute på parkeringsplatsen och försöka komma åt det här nätverket. Så med andra ord så måste jag innan jag ger dig rättigheter måste du authentiseras på något sätt. Det sättet vi har löst det är då med hjälp av en PKI-infrastruktur. Jag vet inte om jag ska gå in på hur PKI fungerar eller jag antar att alla vet vad det är

Japp
Vilket av dem, ska jag gå in på det?

Nej du behöver inte gå in på det
Ok, så vad vi gör är att vi har satt upp en PKI-server som finns inbyggt i Microsoft Windows Server produkter. Där har vi lagt upp en radius-server, radius servern är den som i sin tur då pratar direkt med accesspunkterna, sen har vi delat ut två certifikat till alla våra användare. Ett maskincertifikat och ett användarcertifikat. Det som är smidigt med Microsoft lösningen är då att de här certifikaten kan vi skicka ut till klienterna utan att de behöver göra något speciellt, en så kallad auto enrollement, så att från ena dagen till den andra kan vi ge Microsoft användare säker trådlös access. Det bygger på att både maskinen och användaren authentiserar sig via de här certifikaten som man då har fått. Har man inte rätt maskincertifikat eller användarcertifikat kommer man inte in, och de två måste vara rätt kombination. Jag kan inte ta mitt maskincertifikat och lägga det på en annan dator, eller ta mitt användarcertifikat och logga in med det på en annan dator. Utan de två måste stämma överens om jag vill komma åt nätverket, stämmer de överens har jag den säkra trådlösa accessen.

Sen är det ju också så, precis som du sa innan att jag kanske vill distansarbeta eller sitta på ett café och jobba, då måsta man anta hela tiden att säkerhets boundryn på datorn går ju precis utanför skalet, jag brukar illustrera det med att säga, den här datorn litar jag på, allt utanför litar jag egentligen inte på, så det första jag måste göra är ju att skapa en säker koppling till min arbetsplats, det kan ju som exempel då vara en VPN-lösning. Våran VPN-lösning bygger då på det som kallas smarta kort. Så att om jag då vill komma åt Microsofts nätverk från ett IT-cafe exempel, då måste jag först authentisera mig till Microsoft via mitt smarta kort, sen måste jag genomgå en karantänfunktionalitet som innebär att Microsofts VPN-server kommer från min dator, har du brandväggen på slagen, har du det senaste antiviruset, har du alla säkerhetspatchar som vi vill att du ska ha, för att över huvudtaget få access? Har jag inte det, ja då kommer jag att hamna i karantän, har jag det, ja då kommer jag komma in på vårat nätver**k.** Intressant är att vi har sett en stark trend här efter att vi har erbjudit att våra användare kan komma åt sin mail med RCP via HTTP som det heter. Att vår VPN-användning har sjunkigt drastiskt. För det som personer oftast behöver när de är ute och jobbar på fältet är att just komma åt sin mail. Varför

ska jag behöva VPN för att komma åt mitt arbete, personligen är det extremt sällan jag behöver VPNa in och bli en del av nätverket, för det är ändå det VPN innebär, att just jag blir en del av nätverket. Jo jag kanske skulle behöva komma åt någon intern applikation eller någon intern fil någonstans. Sättet vi har löst det på är att publicera tjänster ut mot nätet, att låta användarna kunna starta sin Outlook direkt, utan att behöva VPNa men ändå på ett enkelt och säkert sätt kunna accessa och hämta sin e-mail. Med detta slipper vi många av de här VPN-scenariorna och det tycker jag är en mycket bättre approach än att få användarna att försöka använda de här VPN funktionaliteterna, ju färre enheter som vi inte har kontroll på som ansluter till vårt nätverk, desto bättre.

En del VPN-lösningar behöver man ju om man har det installerat på burken så att säga bara mata in ett lösenord, Tycker du det är för lite säkerhet för jag menar om datorn blir stulen eller något och de får reda på lösenordet, är det för lite säkerhet att bara behöva authentisera sig så mot företagets nätverk enligt dig?
Ja det där är egentligen inte för mig att säga, det beror på. Säkerhet är ju så att man egentligen kan spendera hur mycket pengar och hur mycket tid som helst på det.Men det viktigaste i slutändan är att man gör det på rätt säkerhet. Rätt säkerhet, det får man endast om du har satt dig ner och funderat på, vad är det jag vill skydda, hur mycket är den data jag vill skydda värd, vad händer om fel personer då får tag på det data jag försöker skydda?

Vad händer då, när jag har klassificerat det här och fått reda på värdet på det, vad vill jag använda för metod, eller vad vill jag använda för resurser för att skydda det här datat. Är det så att jag skulle vilja VPNa in till mitt företag som har publik information på sitt nätverk, det är fem anställda, har inget större krav på säkerhet. Ja då kanske det är rätt säkerhet. Sitter man på Microsofts nätverk, där vi har mycket känslig information som kanske har våra sourcekod på nätverket, med extra skydd då, ja då skulle inte den säkerhetslösningen vara nog

Om man ser på mobilitet och skadlig kod, låt oss säga att jag på något sätt, av någon anledning tar ut min laptop, jag tar med den hem och den blir infekterad på något sätt i hemmanätverket och jag tar in den i företaget sen. Är det ett problem, och hur ska företaget hantera det, finns det skydd? Nu menar jag tekniskt skydd när man väl tar in datorn, vad är det man bör tänka på?
Det viktiga att tänka på här är att det spelar egentligen ingen roll vilka skydd du har implementerat, om skadlig kod körs under administrativa privilegier på din dator, då är det inte din dator längre. Vad man ska fokusera på är att aldrig någonsin få in den här skadliga koden på sin dator. Om man följer några enkla rekommendationer som att ha ditt operativsystem uppdaterat, ha din brandvägg påslagen och ha ett uppdaterat antivirus, då är det ganska liten risk för att man råkar illa ut. Vi vet ju det som att om alla hade slagit på brandväggen i Windows XP hade vi varken haft sasser, blaster eller slammermasken, nu är ju det samma sak, hade alla uppdaterat sitt operativsystem hade vi inte heller haft de där problemen. Men nu är inte det alltid möjligt, man har glömt eller det finns någon annan anledning till varför inte operativsystemen är uppdaterade.

Det är då det primära, se till att man har en patchmanagementstrategi för företaget, och är man en enskild användare på hemmafronten så ska man slå på automatiska uppdateringar då för att få de här uppdateringarna för operativsystemet. Är det ändå att man av någon olycklig anledning får in skadlig kod i systemet, i sin dator, är det ju förhoppningsvis så att anti-viruset ska hjälpa till i det här fallet eller anti-spyware om det nu är någon sådan kod som slunkit in. Hjälper inte det heller och man kanske får in något konstigt i sin dator och tar med den in i företaget, då vill man ju att företaget ska ha någon form av karantän funktionalitet om man ansluter via VPN, tar man väl in datorn till företaget ja då kanske man har ett IDS-system, där man systemet ser till att,

vänta nu varför försöker den här datorn nu prata med alla maskiner samtidigt på alla olika sätt? Då kan det vara en varningslampa. Ifall att man har fått något farligt installerat på sin dator, eller något liknande och inte har ett anti-virus och lyckas infektera sitt företag. Ja då är det ju givetvis så att man måste ha någon form av rutiner på företaget, för vad gör jag om det här händer? Vilka resurser är det jag ska skydda, hur ska jag göra för att bli frisk igen, vad ska jag göra för att undvika det här i framtiden?

Det handlar ju också mångt och mycket om att utbilda sina användare, om att utbilda användarna hur de ska kunna använda datorn på ett säkert sätt, du kan förmana dem på alla sätt och vis med hjälp av policys och procedurer, du kan ge dem tekniska hjälpmedel för att klara sig, men glöm inte att hålla utbildning i incitament om varför ska jag jobba med datorn på ett säkert sätt! Hur väljer jag starka och bra lösenord och vad ska jag tänka på när jag surfar?

En lösenordspolicy tillexempel, hur tycker du personligen, minimunkravet för ett säkert lösenord
Minimunkravet för lösenord i dagsläget är ett så kallat strong password, vi säger strong password då och det består av minst åtta tecken, en stor och en liten bokstav, en siffa och ett alfanumeriskt tecken. Det tar ungefär 14-miljoner år att knäcka, med dagens datorkraft. Det kommer också till en ganska intressant diskussion som jag kan prata om i flera timmar här men, hur hittar jag då på ett sådant här lösenord? Är det svårt att hitta ett ord som är åtta tecken långt och innehåller alla de här kriterierna? Vad jag brukar göra är att hjälpa användarna att hitta starka och långa lösenord som de kan komma ihåg, det finns lite olika formler där, jag brukar säga det att ta en mening istället, att jag var ute och gick med min hund i skogen idag och sen byta ut en bokstav, lägga till en siffra, kanske sätta en punkt på slutet, stor bokstav i meningen, det blir ett extremt starkt lösenord och mycket lättare att komma ihåg än ett 8-tecken långt lösenord.

Sen är det ju så att lösenord är ett problem med tanke på att om du ger tillräckligt mycket med tid, pengar eller datorkraft, så kommer de till slut att knäcka ditt lösenord. Lösningen till det finns i det här är ju att exempel börja använda smarta kort, så att man har identiteten lagrad i sitt smarta kord, med hjälp av ett certifikat och på det sättet kan man då autentisera användarna.

Tack då har vi rett ut lite om lösenord, du nämnde innan säkerhetskopiering, vad är din syn på det hela och används det av företag tillräckligt mycket, vad finns det för problem om man slarvar med säkerhetskopiering, eller slarv av förvaring av backupper?
Ja säkerhetskopiering är något som, ja det beror också lite på då hur stort företaget är och vilken data man har och vad det är man ska skydda, jag rekommenderar då givetvis att man säkerhetskopierar all viktig data och helst ska ju den här vara krypterad och i god kutym bör den också tas off-site så att om mitt hus brinner ner då vill jag ju inte att backupen ska brinna ner med det, utan hantera den säkert på samma sätt du skulle hantera ditt *ljudet föll bort*

Undersökningar har visat att företag är rädda för att uppdatera programsviter och sådant för att de är rädda för nya buggar, är det ett problem och hur ställer ni er till det? Vad kan man göra för att få företagen, för oftast innehåller väl uppdateringarna bra fixar så att säga.
Ja då ska man ju först skilja på en vanlig uppdatering och till exempel en säkerhetsuppdatering. Microsoft har ju valt att en gång i månaden så skickar vi ut säkerhetsuppdateringar till våra kunder, de här säkerhetsuppdateringarna klassificeras på olika sätt då, det kan vara en låg prioritet, en medium prioritet, viktig eller hög, low, middle och critical kallas de. Är det en kritisk säkerhetsuppdatering så rekommenderar vi användarna, eller våra kunder att installera de här säkerhetsuppdateringarna så snart som möjligt.

Är det sådant som ska styras med automatik i en organisation
Automatik i sådant sätt så att man bör ha en procedur, vad ska jag göra med de här uppdateringarna, hur ska jag hantera de här uppdateringarna när jag väl får dem, stora företag har i dag färdiga processer där man då sätter sig ner så fort uppdateringarna kommer, utvärderar dem, börjar testa uppdateringarna, de har alltså en färdig process får hur hanterar jag det här? Nu tappade jag tråden lite vad frågan var.

Det var mer att vi undrade hur i organisationer hur de kan se till att de här säkerhetsuppdateringarna kommer ut till användarna
Ja det beror på då storleken på organisationen, vissa organisationer, små och medelstora företag de kanske då kopplar upp sig direkt mot Windows Update och drar ner uppdateringarna därifrån, medan större företag har då en egen IT organisation som hanterar de här uppdateringarna, tar in dem i sina testsystem, kollar, vad får de för påverkan på vårat företag och därefter ha en utrullningsplan

Vad finns det för stora problem med att hålla tillgänglighet **på informationssystem, någon form av kontinuitetsplan?**
Ja det här är ju lite samma sak som med säkerhet som jag sa innan, man måste bestämma sig hur man ska skydda sin information och det enda sättet man kan göra det är att om man vet vad det är för olika klassificeringar på information, hur viktig är den. Samma fråga kan man ju då ställa sig, hur viktig är det att det här infsystemet finns tillgängligt och vilka krav har vi, är det 99,9 är det 99,99 eller är det 99,99999 osv. Är det så att man har extremt höga krav på ett system ja då får man ju naturligtvis bygga det därefter, det finns ju flera olika lösningar på hur man garanterar upptid på informationssystem, man kan klustra dem, man kan sätta dem i olika former av arrays som det heter och se till att man delar på lasten. Man kan ha olika former av redundant hårdvara, det finns idag företag som garanterar 100% tillgänglighet på Microsoft plattform

Ok då har vi lite information om det, om vi hoppar till standarder och lite kortare frågor, åsikter så avslutar vi sedan med lite MS relaterade och personalrelaterade frågor, låter det bra? Har du tid, det är fredag
Jag har tid, istället för att sitta ute på balkongen nu sitter jag inne i ett mörkt rum

Vad är din generella syn på säkerhetsstandarder som exempelvis ISO 19977
Mmm, det här är ju någonting som vi gillar, det här är riktigt bra, vi har ju valt att bygga någonting som heter Microsoft Security Framework, det finns då alltså ett säkerhetsramverk runt våra produkter som integreras i de olika ISO-standarder som finns idag. Hur driftar man en Microsoft plattform på ett säkert sätt med de olika krav som man har, utan de här standarderna som finns? Det ju väldigt svårt att veta vilken säkerhet har jag idag och vad måste jag göra för att komma till den nivån jag önskar?

Ser du det som att säkerhetsstandarder är till för större organisationer, ISO-standarden är ju väldigt omfattande, småföretag har kanske inte tid eller resurserna och är inte heller i behov av en stor standard, är det enbart för storföretag eller kan småföretag också dra nytta av det?
Man måste vara lite pragmatiskt givetvis om man driver ett mindre företag, samtidigt har vi sett det, vi erbjuder ju någon som heter Security Diagnostic Tool, ett SRV verktyg som man kan ladda ner från vår hemsida, det här är ett gäng enkla frågor som man kan svara på som IT-ansvarig på ett mindre företag och får råd och tipps för att nå den säkerhetnivå som är lämplig för mitt företag. Naturligtvis kan inte det lilla företaget gå igenom en ISO-certifiering med dess lampor, visslor och tutor och funktioner som finns, utan det är ju precis som du säger, något som större företag tittar på, vilken standard måste vi vara compliant på? Det finns företag idag som gör

affärer med stora företag i USA och då kommer Sarbanes-Oxley in och då måste man ju vara compliant mot de standarderna också.

Är standarder lösningar på säkerhetsproblematiken, eller är det bara ett hjälpmedel för att få en högre informationssäkerhet?
Vad är säkerhetsproblematiken?

Ja hur ska man definiera den? Vill du höra vår definition av informationssäkerhet?
Vi brukar säga så här, säkerhet är inte ett mål utan det är en resa. Man kan aldrig göra en säkerhetsfunktion i sitt företag och säga, JA! Nu är vi säkra, ta semester och sedan känna att man aldrig mer behöver titta på det. Säkerhet är något man kontinuerligt måste titta på, utvärdera, vad har vi gjort här, hur har vi gjort här, är det någonting vi behöver ändra på, och det är just det här de här standarderna hjälper till med, att hålla en viss kvalitet. Att man följer en viss funktion som finns beskriven i de här standarderna och där med kan garantera en viss nivå av säkerhet.

Känner du till riktlinjerna BITS exempelvis från krisberedskapsmyndigheten? Basnivå för informationssäkerhet.
Jag har inte läst igenom den, men jag har hört talas om den, BITS på Microsoftspråk betyder Binary Information Transfer System, vilket är en funktion som ser till att inte hela kraften sugs upp av uppdateringar utan man använder bara tillgänglig bandbredd.

Det var ju inte riktigt det, många standarder när de går ner på personal och anställd nivå, definierar ju upp att något som är väldigt viktigt är incidentrapportering. Vad finns det för nytta med det, vad finns det för problem? Användare som inte rapporterar. Utveckla gärna själv
Mm tror inte riktigt jag förstår frågan.

Incidentrapporteringsrutiner, vad kan det bidra till för företagets säkerhet?
Ja pratar man då om funktionalitet idag, något som kallas whistle blower, känner ni till den?

Nej, du får gärna förklara
Ja whistler blower, lite snabbt översatt blir då visselblåsaren. Många företag idag har implementerat funktioner där jag som liten anställd på det stora företaget kan ringa in eller maila in, eller faxa in anonymt och säga det, att här är något som försiggår som jag inte tycker stämmer överens med våra etiska regler eller våra lagar, något som helt enkelt är fel. Det här är något som det finns ett stort mervärde i, en företagsledning är ju intresserade av veta, är det några oegentligheter som försiggår i vårt företag, och i så fall hur ska vi få reda på det här, då finns ju då sådan här funktionalitet som whistle blower.

Menar du om någon anställd bryter, slarvar mot användarpolicyn och sådana grejjer
Absolut, det kan vara allt från sexuella trakasserier till att man gör något som bryter företagets etiska regler, eller helt enkelt lagbrott, att man ser någon oegentlighet som försiggår, någon kopierar data och personer eller, ja vad som helst helt enkelt

Många företag som vi har förstått det, och från min egen erfarenhet, de ger användare tillgång till begränsade rättigheter, begränsade programtillgångar, de får inte installera program och liknande. Men samtidigt verkar många företag inte bry sig om det, hur ser du på det problemet?
Jag ser inte det som ett problem utan mer en trend, för i tiden hade man inte så mycket identiteter som man har idag och det är en problematik för en modern IT-chef får brottas med. Jag har idag på Microsoft som exempel flera identiteter, jag har en identitet för att logga på mitt

nätverk, jag har en identitet för mitt passerkort, jag har en för mitt passerkort, jag har en identitet i vårt HR-system, och så vidare, och så vidare. Alla de här identiteterna har då olika rättigheter till olika system, vem hanterar de olika rättigheterna, vem bestämmer vilka system jag ska ha tillgång till och vem ser då till att när jag kanske byter arbetsuppgifter att rättigheterna tas bort i det systemet som jag fanns i tidigare?

Det som de flesta tittar på idag är precis som du beskriver, hur kan jag se till att användarna har de minsta möjliga rättigheterna som de behöver för att utföra sina arbetsuppgifter, istället för tvärt om som det kanske var tidigare att jag ger alla i mitt företag rättigheter till den här portalen, istället tittar man idag på då att nej ingen ska ha rättighet att komma åt den här portalen utom dom som absolut behöver det, istället får man då be om rättigheter för att komma åt portalen. Då kanske det går ett brev till ens chef som går godkänna, ja Magnus behöver faktiskt tillgång till det här projektet, så har man vänt på pannkakan och då har man implementerat ytterligare ett defense invest lager som jag pratade om tidigare, jag har inte access till de känsliga systemen och skulle min dator då bli smittad på något sätt, ja då kan man inte komma åt dom

Så det tenderar att gå till mer och mer, vad ska man säga behovsstyrda rättigheter och om så är fallet ska det finnas klara och tydliga rutiner, regler om vem som ska besluta om personen ska ha rätt till systemet i företaget, är det så du menar?
Ja det kallas oftast rollbaserade rättigheter, det innebär jag har en funktionsbaserad rättighet, jag har den här rollen, och den här rollen behöver access till det här systemet, eller de här rättigheterna. Sen måste man alltid planera för undantag, annars kommer man misslyckas ganska snabbt

Och det ska styras av några rutiner i företag, så att inte vem som helst kan ge rättigheter då eller
Ja absolut, den grundläggande pelaren i informationsklassificering är att den som skapar datat är den som bestämmer vilken klassificering den ska ha, och sen där efter bygger man strukturerna runt det här. Vem behöver då access till det här, vem ska bestämma vem som ska få access till det. Ett förslag till att lösa det är som vi har valt att lösa det. Behöver jag access till ett system, ja då får jag be om det och beskriva varför jag ska ha access till det, sen måste min chef då eller någon annan i organisationen godkänna mig och se till att jag får rättigheter till det här då.

Anser du att t.ex. sådana här Access kontroll i form av byggnader hör det till informationssäkerhet också? T.ex. som på Ericsson så behöver man ett kort för att komma in i vartenda rum och har man inte kort som kommer man inte in, hör det till informationssäkerhet också, den typen av kontroll alltså fysisk kontroll av, vad skall man säga, rum.
Absolut! Det finns någonting som jag tycker ni skall titta på, om ni går på Microsofts hemsida så finns någonting som heter ”ten immutable laws of security” och en av dem lagarna är att; om jag har fysisk access till ditt system så är det inte ditt system längre. Jag refererade till det tidigare om att om du kör skadlig kod eller om du kör kod och inte har administrativa privilegier så är det inte heller ditt system. Vad jag menar med det första då med om du har fysiska accesser det är att; Kommer jag fram till en server eller till en dator så är det bara en tidsfråga innan jag kommer åt din data. Du kan ju naturligtvis göra det svårare för mig genom att kryptera systemet och använda starka lösenord och ja det finns massa olika system och lösningar. Men har jag möjlighet att sno med mig en server hem då är det en tidsfråga innan jag kan till exempel komma åt din kontodatabas eller din SQL-databas. Jag behöver bara tillräckligt mycket tid pengar eller resurser för att ta mig in i det systemet. Har jag valt att inte skydda det överhuvudtaget så kanske det räcker med att dual bootar med en ny version av operativsystemet och på så sätt kommer åt data. Så ja det fysiska skyddet är en del av säkerhetstänket.

Har det blivit ännu mer intensifierat nu med mer mobila enheter, mobiltelefoner t.ex. din telefon har du din mail i och all den där biten. Finns det numera ett större behov av att även tänka på den fysiska biten av säkerhetsaspekterna?
Absolut! Det är informationsflödet man får fundera på då, var någonstans kommer min information att finnas i mitt företag, ger jag användare bärbara datorer så måste jag ju också ge dem en utbildning för hur skall jag hantera det här och vad skall jag tänka på, hur får jag använda dem och vad bör jag och bör jag inte göra? Vi ser ju en stor efterfrågan för våran mobila plattform på telefoner, som heter Windows mobile, att det skall finnas en möjlighet att kunna sätt ett lösenord på din telefon att om du lägger ifrån dig den och efter fem minuter då så skall telefonen låsa sig automatiskt att du behöver en enkel kanske pinkod eller avancerat lösenord för att kunna använda den. Det som vi också har inbyggd i Windows mobile i våra telefoner är någonting som kallas remote wipe. Har jag då varit ute och festat och kanske glömt telefonen eller tappat bort den eller fått den stulen. Då kan jag kontakta IT-avdelningen och säga det att; tyvärr har jag tappat den här. Då kan de skicka ett så kallat ”poison pill” till din telefon och det gör att den automatiskt ställer sig i factory reset mode alltså all data försvinner från telefonen.

Är det lite samma sak som problematiken som om man går in på ett företag det är människor som inte är vid sina datorer men de är fortfarande påloggade. Hur kan ett företag förhindra att någon obehörig sätter sig ner vid datorn när han är inne i systemet.
Det är då en kombination av dem här sakerna som vi har pratat under den här intervjun. Ett, fysisk access, hur har de kommit in i företaget? Borde inte en person få eskort ifall han kommer in på företaget? Har man lurat sin in via social engineering? Har man access som temporär anställd eller en som har slutat där men fortfarande har access? Det är ju första man måste fråga sig då. Det andra är, har man satt en policy på sina datorer som säger det att efter X antal minuter när jag går från datorn så skall skärmsläckaren gå på med ett lösenord. Eller behöver jag kanske låsa upp datorn med smart kort? Har jag ett system som vi har ett system som vi har på Microsoft då är det ju det att man måste använda sitt smarta kort för att logga på datorn. Samma smarta kort behöver jag för att ta mig igenom de olika dörrarna på företaget vilket innebär att när jag tar ut det smarta kortet så låser sig min arbetsstation automatiskt och då har man ju hindrat det här initiella tillfället att någon bara kan sätta sig ner vid min dator och kanske börja läsa min e-post eller accessa dem system som jag har tillgång till. Sen gäller det ju det att vara skeptisk eller ifrågasättande att om det finns en person in din närhet på ditt företag som du aldrig har sett förut och sitter på någons plats som kanske någon annan brukar sitta på får man gå fram och fråga den personen; Ja hej vem är du, presentera sig, fråga vad gör du här och helt va uppmärksam precis som vilken god medborgare som helst.

Du pratade innan om att det absolut bästa sätt företaget kan ha för att öka medvetandet och kunskapen hos användarna är att kontinuerligt utbilda dem. Men vad har användarna själv för ansvar? Är det liksom människan kanske är lite slarvig eller, vad är dina åsikter om människan, en användares eget ansvar för informationssäkerhet i ett företag som han jobbar på?
Människans ansvar är ju så långt som någon har talat om det för människan man kan inte förvänta sig att alla personer tänker på samma sätt och har samma bakgrund när det gäller informationssäkerhet. Utan en informationsansvarig eller informationssäkerhetschef bör ju fundera på hur gör jag när det kommer nyanställda till företaget? Vilka förutsättningar ger jag mina användare att vara goda medborgare i säkerhetsarbetet? Får de kontinuerlig utbildning om det här att, varför skall jag välja ett starkt lösenord? Hur skall jag hantera min VPN på loggning? Hur fungerar vår säkerhetspolicy har den ändrats eller uppdaterats? Det ger incitament till att få användare att bete sig på ett säkert sätt utbildning är en väldigt viktig del som en del ibland glömmer.

Så att det är utbildning som är det absolut viktigaste då för ett företag när det gäller riskerna med användarna?
Nja säkerhet är lite som en kedja, lägger du jättemycket krut på en jättestor och fin fet brandvägg, men ingen krut någonting annat då står ju någon där och häckar inne på ditt företag och tar din dator. Lägger du all teknik på utbildning och utbilda användarna men ingenting på patch management strategier och se till att dina system är uppdaterade, ja då kommer det att fallera på det också. Likaväl, lägger du väldigt mycket teknik på det hela men ingen utbildning ja då vet kanske inte användarna hur de skall använda systemen eller så försöker de göra allting i sin makt för att gå runt de säkerhetsinstruktioner eller policys som finns.

Du pratade innan om att det kan vara problem om människa har slutat men fortfarande har access till vissa saker. Är det också i så fall så då en ledningsfråga att man måste ha klara rutiner för att; ok när jag anställer jag en människa så skall han genomgå dem här testerna vi skall kolla på honom och undersöka honom. Och när han slutar skall det finnas rutiner för vad som händer med hans information.
Säkerhet är ju en ledningsfråga, den som är ansvarig ifall det händer någonting är ju just via jobb på företaget. Sen kommer ju den personen inte hantera det här utan oftast att revidera det till en annan person. När det gäller hantering användare, så gäller det ju ha en tydlig policy, vad skall jag göra när en användare börjar på mitt företag och vad skall jag göra när en användare slutar? Man bör ju ha någon form exit-intervju ifall man kan kalla det så. Att, hur skall jag göra, vem har ansvar för de olika systemen och vem bestämmer över de olika systemen? Kanske inte var så tydligt men jag tror att du förstår vad jag menar.

Jag förstår vad du menar. Internetanvändandet har ju ökat något enormt vi är alltid uppkopplade i västvärlden på väldigt många arbetsplatser. Vilka problem medför det? Kan du fundera lite runt just Internet användningen där.
Jag tycker Internet är en otrolig möjlighet och det gör det att många kan till exempel sitta och jobba hemma eller på distans. Så att kunna använda Internet på rätt sätt är en fantastisk möjlighet som jag tycker att alla skall utforska. Jag sitter mycket hellre hemma och gör mina bankärenden än att behöva gå in till en bank och stå i kö och vänta och prata, vilket iofs. är trevligt att prata med olika personer men, kan jag göra det hemifrån så blir jag mycket gladare. Sen att kunna kanske handla någonting på en aktionssite eller beställa ett nytt kylskåp från ett företag är för mig mycket bekvämare än att behöva gå till en firma och gå runt och titta på dem och behöva baxa hem själv.

Riskerna med Internetanvändning, vad är enligt dig och i din yrkeskarriär eller din arbetsroll. Vad är dina åsikter om de största riskerna med att just det att användare använder Internet väldigt mycket.
Det finns illvilliga användare på Internet, eftersom alla kan använda det och man kan nå väldigt många personer väldigt fort så är det här ju till exempel som phising kan ju vara ett stort problem. Alltså man skickar ut spam att du får ett mail som det står att; hej det är från bank vi tror att någon har accessat ditt konto vänlig och klicka på den här länken och följ procedurerna som står på hemsidan. Som en hemanvändare med begränsade datorkunskaper då så kanske man tror på det här klickar på länken och kommer till en hemsida som egentligen är hostad av illvilliga personer som i sin tur vill lura av dig din kontoinformation eller ditt visakorts-nummer och liknande saker. Och därmed kunna använda det och ta pengar ifrån dig t.ex. Så att en sak där är ju, Microsoft har till exempel varit med tillsammans med IST och andra företag och gjort en kampanj som heter Surfa Lugnt, känner ni till den?

Ja beredskapsmyndigheten har också någonting med den att göra tror jag.

Precis, där vi har gått ut med på bred fornt tillsammans med flera olika företag och gett guidelines och information om vad man skall tänka när man är ute på Internet. Själv brukar ju jag ge dem här rekommendationerna som jag sa innan. Se till att ditt operativsystem är uppdaterat, kör med en brandvägg på och se till att du har ett uppdaterat antivirus program.

Det finns ju många sårbarheter i webbläsare också, är det det du menar med operativsystem att man skall se till att ha uppdaterade versioner av webbläsarna.
Ja i Windows så följer det ju med en webbläsare, Internet explorer, håller man sitt operativsystem uppdaterat så ingår ju uppdateringar för Internet explorer i det. Har man valt någon annan webbläsare, då gäller det ju att separat se till att den är uppdaterad också. Det här är någonting som man ibland kanske glömmer då att se till att ha alla dem program som man använder på sin dator uppdaterade. Microsoft använder ju den här tjänsten som heter automatic update, så har man installerat Windows XP med service pack 2 då har vi slagit på automatiska uppdateringar åt dig som användare. Med andra ord så kommer din dator automatiskt uppdateras så fort det finns några säkerhetsuppdateringar tillängliga. Det tillsammans med brandvägg och antivirus och ett sunt förnuft när man surfar då är man i goda händer.

Ok till exempel en uppdaterad webbläsare vilka hot skyddar den mot?
Jag tror inte jag förstår frågan.

Vad finns det för farligheter eller skadlig kod som kan komma in i din dator om man inte har en uppdaterad webbläsare?
Ja, alltså alla webbläsare som finns på marknaden behöver ju uppdateras oavsett vilket märke eller smak det är. Ifall man inte har en uppdaterad webbläsare då spelar det ingen roll vilken version man kör då kan man ändå råka illa ut. Det man skall veta är det att de vanliga siterna, aftonbladet, expressen, din bank och alla de här sportsiterna som du kanske är inne på. Det är inte dem som är problemet. Problemet är de som inte har några skrupler, som tillverkar de lite mörkare sidorna på Internet. Att det vanligaste sättet att få in skadlig kod i datorn är ju att man surfar på någon skum sida eller att man kanske installerar en exe-fil som man får tillskickad på sig på det ena eller andra sättet. Kanske laddar ner något program från någon skum site eller får den från någon kompis som du inte vet var den kommer ifrån och om den har blivit infekterad.

Om man till exempel ska slänga en hårddisk, har man ju hört att informationen egentligen inte är raderad. Amerikanska armen hade slängt hårddiskar i Afghanistan som senare såldes med känslig information på en marknad inte långt ifrån. Är det ett stort problem och är företagen verkligen medvetna om dem?
De större företagen har ju oftast en policy, hur skrotar vi hårdvara t.ex. hårddiskar då och allt som oftast har en form av logisk överskridning till exempel i Windows finns det redan ett kommando som heter ”Cipher” som man kan använda för att skriva över data väldigt många gånger och sen tömmer man datorn så skriver man över med slumpmässig data och nollar den och håller på sådär. Sen då kan man sätta en yxa i hårddisken för att avsluta det hela. Om man är riktigt paranoid så ska ju hårddisken malas ner till finspån.

***Skratt* Det är inte så vanligt va?**
Det beror på vilken säkerhetskategorisering är det? Då är det så att jobbar man med väldigt hemlig data då kostar det om datan kommer i fel händer då kanske den här extra kostnaden för nya hårddiskar är en ganska liten kostnad i jämförelse med den kostnaden eller den risken som du får ifall datan hamnar i fel händer. Ifall det är en person som bara jobbar men publik data hela tiden och sen kanske köper en ny laptop eller liknande då kan det räcka med att bara skriva över hårddisken och det skulle inte vara någon större katastrof om någon skulle försöka återskapa datan för då är det aldeles för jobbigt i förhållandet till det värdet datan har.

Så det är fortfarande det där, en fråga om informationsklassning igen då?
Det är processer för hur skall jag göra med del olika delarna som jag har i mitt företag egentligen vilket värde ar det jag håller på med egentligen och har jag använt rätt säkerhetstänk för det här?

Varför jag skratta var att någon i den amerikanska armén måste ha missat det, för jag misstänker att de har en sådan policy om information. Att är det känslig information så skall den förstöras och enligt dig är det en utbildningsfråga i det läget troligtvis då. Nu kanske inte du kan säga om det specifika fallet men rent generellt sätt så borde det vara en utbildningsfråga att den här personen kanske inte förstod eller hade hört om policyn tillräckligt mycket.
Precis det kan vara exakt det som du säger å ena sidan kanske det var någon som aldrig har talat om det för den här personen att det här förväntas att du göra. Alternativt så har man talat om det för den här personen men det var väldigt längesedan och man glömmer bort det, det händer man är ju inte mer än människa. Ett annat alternativ är jag skiter i det som anställd, jag struntar helt enkelt i policyn och sen visar det sig att det här händer då o ja då är det dags att gå längst ut på straffskalan då att det får rättsliga följder då för det man har gjort.

Är det tekniken eller organisationen som är svårast att hantera när det kommer till informationssäkerhet? Enligt din egen uppfattning.
Det ena skulle aldrig funka utan det andra.

Så det är en kombination?
Ja. Så får man välja att lite för mycket på det ena eller lite för mycket på det andra. De säkerhetschefer som lyckas bäst är den som har lite kunskap i alla delar av det vi har pratat om.

Ok, en liten tanke som vi har fått via viss litteratur är: Rent tekniskt har säkerhet vart ett problem längre än det har varit organisatoriskt i och med att vi snabbt har blivit ”ihopkopplade” i ett enda stort nät och i och med det har det tillkommit mer problem kring just organisationen. Man vet t.ex. idag hur man gör säkra brandväggar det är något man kan ta på medan organisationen kan uppfattas som något mer svårhanterligt. Har du några tankar om det?
Det är naturligtvis så att för att man skall lyckas i det här så är det så att de verktyg man ger sina anställda måste man ju få hjälp med hur jag skall använda dem här. Idag måste man ju gå en utbildning för att få ett körkort och sen måste man genomgå ett prov. I datavärlden är det ju inte så kan vem som helst kasta sig ut på Internet och blåsa iväg. För att lyckas att inte råka illa ut då finns det några saker som man måste tänka på och med hjälp av olika kurser olika informationssätt, när ni skriver den här uppsatsen, när vi är ute o pratar med kunder, när andra säkerhetsföretag informerar. All information gör ju att användarna tar till sig det här och som jag sa innan då för företag så gäller det ju för företagen att utbilda användare det här är ett verktyg som ni får av oss och här är sättet som vi förväntar er att använda det kan finnas några fallgropar och så hjälper man till och identifierar dem och har du några frågor eller inte vet vad du skall göra så fråga då hellre en gång för mycket än en gång för lite.

Ok, om vi tar en Microsoft-relaterad fråga så har ni blivit väldigt kritiserade för säkerhetsbrister, mycket på grund av att ni används av väldigt många personer och har stor programsvit. Hur bemöter ni sådan kritik och vad är era tankar om det?
Microsoft har ju inte haft det bästa säkerhetsryktet, precis som du säger då, det här identifierades då år 2002 ganska konkret då av vår grundare Bill Gates. Då startade han någonting som heter trustworthy computing. trustworthy computing innehåller fyra pelare, en är säkerhet, en är tillänglighet en är buisness integrity och en är privacy. Om man inte har en strategi och alla de här

fyra pelarna då har man egentligen ingen säkerhet. Det spelar ingen hur säkert jag gör ett system om jag inte har någon strategi för vilka som skall ha access till den. Är det ett jättesäkert system och jag vet jag vem som skall ha acess till det, finns den inte tillänglig så spelar det inte heller någon roll.

Det sista då med buisness integrity så handlar det då om standarder, det gäller att följa de standarder som finns ute i världen. Det här är någonting vi började jobba med 2002 och vi dessutom gjorde var att vi satte någonting som heter ”secure development lifecycle” och det här är någonting som jag pratade om i början då att det här behöver man ta med. Att man måste se till att man utvecklar programvaran på ett säkert sätt. Tidigare har inte säkerhet kommit i första rummet när det gäller Microsoft programvaran det har kanske varit funktionalitet eller användarvänlighet som vi har satt i det första rummet. Där gjorde man då en ändring och sa att. Nej vi måste sätta säkerhet högst på prioriteringslistan nu och göra en ändring i det här för vi ser att det här håller på att barka åt fel håll. Den första produkten som kom ut efter den här säkerhetssatsningen då och utbildningen av våra programmerare, testare och våra utvecklare var XP service pack 2. När det gäller XP service pack 2 så vet jag att det finns vissa företag som har haft problem att installera det, det finns företag som har lyckats väldigt bra och det finn användare knappt har märkt att det har installerat XP service pack 2. Men det är data applicerat dem som ansluter till Windows update för att hämta nya uppdateringar, så är det ungefär 15 gånger mindre chans för att få skadlig kod på sin dator än om man har någon tidigare version av Windows. Det är ett kvitto på att man börjar bättra sig ganska bra den första produkten, hela produkten, som kommer att komma av den här secure Development lifecycle är vår nästa end-produkt som heter Windows Vista och där har man gjort några radikala förändringar när det gäller säkerhetstänket bland annan har man sagt det att, nej vi skall ge möjligheten för användarna att inte behöva vara administratör hela tiden. Mycket skulle se annorlunda ut i dagens säkerhetsvärld om ifall en windows användare behövde vara administratör och kanske håller på att surfa runt på webben som administratör hela tiden. Så att där har man gett en möjlighet med en funktion som heter user account control att en användare kan vara en användare hela tiden och när man behöver göra en administrativ manöver kanske byta klockan eller installera någon service komponent eller vidare, ja då får man fylla i de administrativa privilegierarna sen blir man administratör för endast den korta stunden som man behöver göra det administrativa sen är man tillbaka som vanlig användare. Tillsammans med Internet Explorer 7 då som kommer i Windows Vista där man har gjort en stor förändring som man kallar Internet Explorer protected Mode. De innebär att man vi har skapat en ny användare i Vista som har lägre rättigheter än någon annan användare. Idag kan man säga att man har tre rättigheter i Windows XP. Det finns, Admin, User och Guest där guest använder man ju knappt så det finns admin och user. Men de flesta användare är tyvärr idag fortfarande administratörer på sina maskiner utom vissa företag då som har låst ner systemen eller sänkt rättigheterna då ner till användarnivå. I Vista så skapar vi användare som har ännu färre rättigheter än vad gästanvändaren har. Den här användaren har två rättigheter egentligen. Man kan skriva till temporary Internet files och man kan skriva till favorites. Under den här användarens rättigheter startar vi alltid Internet Explorer så även om jag skulle vara administratör så kommer Internet Explorer att köra med väldigt begränsade privilegier. Samt göra det att om det då dyker upp en säkerhetslucka som försöker skriva ner sig själv på hårddisken eller ändra någonting i registret eller försöker göra någonting i systemet så kommer den inte få dem rättigheterna helt enkelt.
Dom som jag skulle vilja tillägga är också att Microsoft har fått den högsta kommersiella säkerehtscertifieringen av sitt operativsystem Windows XP (Sp2) + Windows Server 2003. Mer info här: http://www.microsoft.com/presspass/press/2005/dec05/12-14CommonCriteriaPR.mspx

Det var ett bra och långt och uttömmande svar på min fråga.

Det var en kort fem minuters version av min en-timmes presentation om vad Microsoft gör i området säkerhet.

Vad hände med Palladium egentligen?
Palladium då gick ju över i någonting som heter NGSCB, Next Generation Secure Computing Base. Och den i sin tur ser vi en liten funktionalitet i vista också i någonting som heter bitlocker. Bitlocker är någonting som ger möjligheten att kryptera en hel volym. I Windows 2000 och framåt har vi haft någonting heter EPS som står för Encrypted File System där du kan kryptera en enskild fil eller mapp. Men i Vista ger vi dig möjligheten att kryptera en hel volym istället. I fall man nu vill göra det här på ett riktigt säkert och transparent sett så kan man köpa en Vista-dator med ett såkallat TPM-chip i och det står för Trusted Platform Module. Vad det innebär är att, istället för att lagra certifikaten på hårddisken så lagras certifikatet för att dekryptera den hör volymen i hårdvara. Ett problem man har idag är att mjukvara kan alltid manipuleras av mjukvara. Har jag min lösenords hasch så är det ju bara en fråga om tid, pengar och resurser som jag sa innan för att jag kan knäcka den och kan jag inte komma åt mitt certifikat ja då blir det ju väldigt svårt att knäcka den. Och vad det här TPN-chipet gör då att när datorn bootar så frågar operativsystem det här att ja jag behöver en nyckel här för att kunna fortsätta läsa på hårddisken för nu är det bara krypterad data här. Jämför sitt certifikat med det certifikatet som finns i hårdvara, stämmer de här överens ja då kommer operativsystemet att fortsätta boota och då kommer jag kunna komma åt min data. Har jag då tagit den här hårddisken och flyttat över till en annan maskin eller på något annat sätt manipulerat data, så kommer inte datan att boota helt enkelt och då kommer jag inte att kunna komma åt min data.
Jag vill också nämna att det är inte Microsoft som är den enda initivativtagaren till NGSCB utan det är en organisation. (Mer info här: https://www.**trusted**d**computinggroup**.org/)

Tror du att det är framtidens väg?
Ja, jag tror att för dem företag som hanterar känsliga data eller användare som hanterar känslig data då är ju det här ett sätt att skydda sig. Det finns ju idag företag som betalar en hel del i andra licenskostnader för att kryptera sina data. Då har vi, erbjuder vi ett alternativ här som med alla säkerhetslösningar när det gäller t.ex. brandväggar, virus, viruslösningar eller vad nu det må vara. Så säger jag, använd det som passar dig bäst, använd den lösning som är effektivast för och mest kostnadseffektiv. De här behoven är ju olika från företag till företag eller från användare till användare, vi erbjuder en lösning.

Ok, för att summera upp lite, skall bara kolla om jag har förstått dig rätt. Informationssäkerhet är ett så pass komplext problem för att det dels består av teknik och människor.
Och processer.

Och processer ja, tack, Nu tappade jag tråden lite vi kör en annan fråga så länge. Har du själv blivit drabbad av t.ex. illvillig kod?
Jag försöker tänka tillbaka det att ja när jag hade min Amiga 500 så fick jag en gång ett virus som gjorde att det dök upp smiley för en sekund sen försvann den i min dator. Jag förstod aldrig riktigt vad det var men nu i backspegeln sådär så vet jag ju då vad det var för någonting och jag vet dessutom hur den dök upp i min dator och det var ju naturligtvis mitt egna fel då att jag hade installerat ett program som jag inte visste var det kom ifrån, en osäker källa då. I dagsläget så har jag ju lite mer kunskaper än vad jag hade på den tiden så att nu mera när jag kör ett operativsystem som är uppdaterat jag har mitt antivirus påslaget, jag har min brandvägg på och jag är naturligt skeptiskt när folk skickar mig länkar eller filer hela tiden då. Då hoppas jag att jag naturligtvis inte skall råka ut för någonting konstigt, men 100 % säkerhet det är någonting som antigen är en utopi eller så blir det väldigt oanvändbart eller väldigt dyrt det systemet.

Så att om man har för hög säkerhet så kan användaren inte utföra sina uppgifter på en organisation är det så man kan dra det, om man hårddrar det? Är det så du menar?
Ja, om jag skulle ge användarna, ställa det krav så att du behöver ett 127 tecken långt lösenord som du behöver byta det varje dag. Då skulle du antagligen inte bli så glad på mig.

Förmodligen inte.
Det skulle vara väldigt svårt för en hackare att försöka lista ut vilka lösenord det var om det inte slutar med att alla användare antigen gjorde uppror eller skriver ner lösenorden bredvid sin dator varje dag. Så att säkerhet är hela tiden en balansgång och det viktigaste är att man använder rätt säkerhet.

Om man ser det på att i och med att det är ökat användande av mobil hårdvara. Om jag har förstått dig rätt så har inte problematiken eller vad skall man säga, grundproblematiken är fortfarande den samma men den kan ha intensifierats för att man använder Internet mer och mer. Men säkerhetsproblemen som har funnits inom säkerhet just när det gäller datoranvändande och en användare de är dem samma.
Ja jag ser ju det här med mobilitet som en möjlighet och inte som ett problem. Det här ger möjlighet för användarna att jobba hemifrån och möjlighet för mig att kontrollera min e-post via ett Internet café på min corporate laptop. Möjligheten för mig att läsa min e-post på min telefon när jag är på en flygplats i valfritt land det är ju en fantastisk möjlighet och det gäller ju att hålla tungan rätt i munnen när man ger de här möjligheterna till sina användare och ge dem rätt utbildning och ge dem enkla och användbara regler, policyn, verktyg för det här. Då finns det alla möjligheter att lyckas med en mobil strategi.

Ok en avslutande fråga, eller det är två frågor rättare sagt. Vad är ditt bästa tips till en användare respektive en säkerhetsansvarig ur ett säkerhetsperspektiv?
Tipset till användare först då, de här tre sakerna som jag sa då. Ett, håll ditt operativsystem uppdaterat, se till att ha en brandvägg påslagen, se till att ha ett uppdaterat antivirus och surfa lugnt, var försiktig med vilka sidor du besöker, var skeptiskt mot folk som försöker skicka filer till dig och installera aldrig program som du inte vet var det kommer ifrån eller var de har varit. När det gäller företaget så skulle jag vilja säga; Ha en klar och tydlig strategi för hur man uppdaterar sina datorer. Vad skall jag göra när det kommer säkerhetsuppdateringar, från alla leverantörer inte bara Microsoft. Hur hanterar jag dem uppdateringar som kommer? Har jag någon strategi ifall jag behöver väldigt snabbt göra någonting på mitt företag ifall jag behöver skicka en uppdatering inom 24 timmar, hur skall jag göra det? Vem är ansvarig för det här och framför allt se till att kunna följa upp det här när jag väl har lagt ut mina uppdateringar. Hur vet jag att det har kommit ut på mina system. Sen gäller det ju då att som jag sa att hålla utbildning för användarna vad de skall göra vad skall de inte göra, ha en enkel och tydlig policy på max en sida, som användarna få gå igenom med jämna mellanrum och ge en möjlighet att återmata till sin chef eller till organisationen ifall det är någonting som man inte förstår eller ifall man ser något som är konstigt som vi pratade om innan då. Är det ett större företag så bör man följa de ISO standarder vi har pratat om innan.

Då var vi klara med frågorna eller frågegrupperna, du skall ha ett otroligt stort tack!
Tack själv.

Bilaga 4, Expertintervju Per Hellqvist, Symantec Nordic AB

Kort presentation om bakgrunden till intervjun.

Om du kan börja och nämna lite om dina arbetsuppgifter på Symantec.
Jag arbetar som säkerhetsspeciallist det går ut mycket på samla information och undervisa andra, lite evangeliserande om nya hot som dyker upp och om säkerhetsproblemantiken som finns därute.

I takt med att mobilitet har ökat på företag och organisationer, har säkerhetsbehoven ökat tycker du?
Ja absolut. Problemet idag är ju att alla som arbetar med IT-säkerhet och informationsfrågor behöver ju veta vart informationen finns vid varje givet tillfälle. Det finns inga idag som kan säga att de vet var all information finns var det hanteras, vart det överförs och vart det accessas. För att idag så finns det så många enheter som är uppkopplade mot nätverk eller många enheter som man använder för att överföra, lagra och hantera informationen. Du har ju skalan ifrån desktop till laptop till mobila enheter, blackberrys och allt möjligt sådant där. Man skjuter ut information hela tiden i samband att man synkar e-posten eller man tar med sig filer från jobbet för att försöka jobba på Arlanda och springer omkring med företagets information överallt och hela tiden. Och det gör ju då att man måste skydda informationen överallt och hela tiden, så att man vet ju som sagt inte var den finns och var den hanteras och vilken information det är som handtags av vem. Så idag är det enormt svart hål bara för dem som skall skydda informationen. Det är det att de måste veta detta, man får anta det värsta så att det går att skydda informationen. Kanske nästan mer än det behövs eftersom man inte vet vilken klassning man har på informationen som finns därute måste man anta det värsta och egentligen ta i med hårdhandskarna och det är här man ligger långt efter idag. Man har inte riktigt fått in det här med mobiliteten i sina säkerhets-policys och det är ju det att anställda inte vet vilka regler som gäller man kanske inte har programvaror och rutiner för att hantera informationen.

Du nämnde klassificering, vad menar du med det?
All information som hanteras på företaget måste klassificeras på något sätt om det öppen information som alla kan ta del av, som man lägger upp på webbsidor, om det är intern information eller om det är hemlig information, alltså i företaget internt klassificerad information. Problemen för företagen idag är att man slutade med detta för en massa år sedan. Det gör ju det att man inte vet vilken information som är hemlig och vilken som är öppen och företagets anställda sitter och chattar via MSN eller Yahoo om man inte skickar en fil via mailen så skickar man det via Chattprogram eller något sånt där, man vet inte vilken säkerhetsgrad informationen har. Det andra problemet man får är, man vet inte vad man måste ta backup på eftersom man inte vet vilka maskiner som håller riktigt känslig data så måste man ta backup på allting. Och då blir det stort för då får man med Mp3-filer och semesterbilder och allt sådant där

Tror du att bekvämligheten spelar roll i det här fallet. Till exempel det att det är ganska enkelt att stoppa in ett USB-minne eller någonting alltså att man inte tänker på riskerna det kan medföra.
Det finns ju jättemånga fall där säljchefen har köpt nya prylar till sina anställda eller man USB-minnen som giveaways eller någonting sånt där, så man använder ny teknik bara för att det går. Och IT-avdelningen kanske inte har blivit underättade om det så man får saker i händer där ute. Och så är det ju såklart desto enklare någonting är att använda desto större är chansen eller risken att man använder den.

Du nämnde innan kryptering på information och sådana saker. Vad är dina tankar om just kryptering till exempel på hårddiskar, just med bärbara enheter jag vet att telefoner kanske inte går att kryptera så enkelt, informationen som ligger på den.
Jodå, det finns ju program för nästan allting, sen om man litar på programmet är en annan sak. Det finns ju jättemycket att ladda ner från Internet. Men det är ju absolut det viktigaste om man kör laptops och mobila enheter om man skall släpa runt på företagets känsliga information då måste den skyddas och det bästa och enklaste sättet för att skydda informationen är ju just kryptering. Så om du tappar bort ett minnekort eller en laptop så har ju den som hittar prylen all tid i världen på sig att ta del av informationen. Om den då inte är krypterad så är den ju egentligen helt öppen. Om du slänger ner en massa saker på ett minneskort eller mobiltelefon eller någonting och tappar bort minneskortet så kan ju vem som helst plocka upp den och stoppa in det i sin mobiltelefon och sen ta del av informationen, så kryptering är det absolut viktigaste idag.

Hur märker du bland företag kryptering är det vanligt att de krypterar information på bärbara enheter.
Skratt Nej, laptops är ju vanligare än mobiltelefoner men det är fortfarande inte vanligt.

Vilka mobila enheter medför störst risker för företagen idag enligt dig.
Det beror på vad du menar med risk, vi har ju allt idag från elak kod till stöld och glömma bort i taxin.

OK, rent generellt sätt var har företagen minst koll när det gäller mobila enheter?
Ja det är ju mobiltelefonerna och PDA och sådant där. Stöldbegärligheten är enorm på de. Man står på krogen och lägger upp mobiltelefonen på disken eller på bordet och så står man och dricker en bärs o vänder ryggen till och sen när man vänder sig tillbaka så är mobiltelefonen borta. Eller också så glömmer man bort den eller den trillar ur fickan i taxin på väg till Arlanda och all information som ligger på den är borta. Har man då synkat e-posten och har kundinformation eller annan känslig information så är ju den också borta. På laptops har man i alla fall den här lilla Windows inloggningen till skydd, den räcker inte långt med det är nån slags säkerhet va. Men på mobiltelefoner har man ingen koll alls.

Ok, du sa innan illvillig kod bland annat, är det ett problem som ökar i omfattning i och med man kanske tar hem sin dator och får den smittad?
Menar du Laptops eller Mobiltelefoner?

Laptops.
Med laptops har du problemet, många företag har byggt upp sin säkerhet enligt äggprincipen. Man har ett ganska starkt perimeterskydd på kontoret men sen om någon tar med sig laptopen utanför kontorets skyddande väggar och skyddande perimeterskydd. Så har man egentligen inget skydd på själva bärbara datorn man kanske har ett antivirusprogram installerat. När man då åker ut till Arlanda eller man sätter sig hemma och jobbar och kopplar upp sig eller kopplar upp sig via

trådlösa nätverk någonstans. Så är man rakt ut på Internet då och har man inte då en personlig brandvägg med sig på laptopen så är man ju helt oskyddad. Jag har just idag besökt ett företag där man egentligen bara har ett antivirus program på sina bärbara datorer. Man tillåter trådlösa uppkopplingar helt utan personliga brandväggar och det gör ju då att datorn är vidöppen för alla.

Wlan t.ex., trådlöst nät, medför det ökad problemantik också, den typen av ny teknik?
Ja det gör det eftersom trafiken skickas ju fritt i luften med vanlig radiotrafik och krypteringen om den ens är påslagen är väldigt bristfällig.

Menar du WEP?
Ja precis, WEP krypteringen är usel. Kör man inte t.ex. en VPN koppling så måste man anta att informationen kan spelas in och avlyssnas. Det finns en hel radda med andra attack metoder mot trådlösa nätverk. Till exempel kan man ju sänka ett företags nätverk med en baby monitor som man har modifierat.

Hur fungerar det?
Det trådlösa nätverket sänder på samma frekvensband som mikrovågsugnar, babymonitorer, trådlösa telefoner och annat så kan man ju störa ytterfrekvensbandet genom att modifiera enheten. På flera företag går hastigheten på det trådlösa nätverket ner runt lunchtid när står och värmer sina matlådor, mikrovågsugnarna stör ut den trådlösa trafiken.

Beredskapsmyndigheten nämnde till exempel ip-telefoni och att många företag är lite rädda för att börja använda ip-telefoni på grund av säkerhetsrisken men de är inte rädda att börja använda trådlösa nätverk på grund av säkerhetsrisker då.
Ja det är jättekonstigt, men många företag just nu är så att det är dyrt som tusan att dra sladd. Det är mycket billigare att ha trådlösa nätverk för då kan ju företagets anställda sätta sig varsomhelst som arbetsgrupper och börja eller i konferensrum och sådant där, så är det ju lite smidigare med trådlöst än att hålla på och dra sladdar. Allting sådant övergränser tydligen behovet av säkerhet då, vilket är ett problem.

Magnus Lindqvist på Microsoft han ansåg att trådlösa nät är enklare eller det är säkrare så att säga än trådade nät. På grund av att om man kommer in i en reception finns det oftast ett nätverksuttag man kan komma åt medan om man har ett välskyddat trådlöst när är det mycket mycket säkrare.
Det får stå för honom. Men allting handlar ju om hur man konfigurerar nätverket man kan ju göra samma sak mer trådlösa nätverk som med trådbundna nätverk bara det att med trådlösa nätverk har du problemet att allting skickas med radiotrafik 100 meter åt alla håll. Har man allting i trådbundna nätverk så vet du var nätverket börjar och slutar i princip, på ett bättre sätt än man gör med trådlösa nätverk. Med riktade antenner och sådant där kan man ju komma åt trådlösa nätverk på många 100 meters avstånd. Med trådade nätverk en fysisk närhet.

Vad bör ett för att förhindra att illvillig kod i systemet om de använder mycket distansarbete och människor tar hem sina datorer osv.
Man måste se till att skydda datorerna och framförallt informationen då där den hanteras lagras och överförs. Det innebär att man måste bära med sig skyddet hela tiden alltså skydda enheten där du har informationen och sen skydda överföringen. Jag brukar predika skillnaden mellan äggsäkerhet och löksäkerhet. För med äggsäkerhet har man det här parimeterskyddet med en stor brandvägg och ett antivirusprogram med gateway och så vidare. Och då räcker det med att ett mail med en bifogad fil kommer igenom för att allting skall infekteras inne på företaget för där är allting mjuk och mysigt precis som när man knäcker ett ägg. Om man har löksäkerhet har man lager på lager med säkerhet utanpå varandra som för att säkra kärnan täcker upp och skyddar. Så

det spelar ingen roll om någonting kommer igenom parimeterskyddet eller om jag tar min laptop eller mobiltelefon ut från företagen och sätter mig utanför och jobbar, så jag bär med mig säkerheten, jag bär med mig flera lager av säkerhet utanpå varandra som täcker upp för varandra så att säga. Så har man tänkt sig på en laptop så kör man antivirus program, personlig brandvägg och en IDS plus krypteringarna för flera olika säkerhetstekniker som täcker upp för varandra.

Du nämnde innan säkerhetskopiering, backuper. Används det tillräckligt mycket bland företag? Du pratade innan även om att man vet inte riktigt hur man skall klassificera information så man säkerhetskopierar allting. Har det behovet också ökat i takt med att vi har fått större hårddiskar på bärbara enheter.
Det här är ju ett galloperande problem det blir ju aldrig bättre. Och vad gäller backuptagninar så är det oerhört olika ute på företagen, det gemensamma problemet vi har idag är just det att vi inte vet och, de anställda framförallt inte vet, hur man får klassificera informationen och det finns inga klara regler och riktlinjer. Jag var nere och pratade för någon månad sen i Göteborg inför en grupp, CIO, och beskrev just den här problematiken eftersom man inte vet vilken information som är känslig tvingas man att ta backup på allting och det kostar jättemycket diskyta, det blir en dyr lösning. Och de bara sitter och nickar och håller med, japp så gör vi, köp mer disk *skratt*. Man har inget bra sätt idag att klassificera information eller det finns inget bra system att på ett automatiskt sätt avgöra vilken information skall ha vilken klassning. Och gör att de anställda måste tvinga ta ställning hela tiden och det räcker med att man missar på ett ställe för att det skall bli fel i strängen. Men det stora problemet yttrar ju sig i då att man tvingas ta backup på allting då egentligen och det är dyrt.

Om vi hoppar in då på standarder för de kan ju hjälpa till att klassificera information. Vad är din syn på säkerhetsstandarder som t.ex. ISO eller liknande.
Jag har faktiskt inte studerat de bitarna alls. På pappret ser det ganska lätt ut när det gäller klassificering, jag menar öppen information, är sådan information som man kan publicera på webben eller det gör ingenting om det står om det i kvällstidningarna. Intern information som kan var känslig om den kommer ut eller kan vara till nytta för konkurrenterna eller det kan vara pinsamt om det hamnar i kvällstidningen. Och hemlig information är sådant som absolut inte får komma ut och det är katastrof om det hamnar i kvällstidningen. Så det är liksom en ganska enkel tankebild man har, liksom när man hanterar informationen och vad skulle hända om det här kommer ut. Men när man sitter och jobbar med saker dag in och dag ut så är det ganska lätt att glömma bort, det där svårt att hålla disciplinen uppe. Därför vore det bra med ett nästan automatiskt system som tog hand om det där åt de anställda, annars är man ju åter igen tillbaka i problemet.

Du pratade innan om policys ifrån organisationen från organisationen som skall styra vad användarna skall göra och sådant. Vad menar du då?
Ja då pratar vi om mobiltelefoner och sådana saker eller?

Exakt mobiltelefoner hur användarna skall bete sig.
När jag är ute och håller föreläsningar så brukar jag ge sådana här enkla tips och tricks som en administratör ändå kan bära med sig och när det gäller mobiltelefoner och informationshantering så har jag den här enkla frågan; Vem får har vilken information på vilken enhet? Om man tänker igenom den frågan när någon anställd kommer och vill göra någonting så kommer man väldigt långt. För det första man tänker på är vem är personen vad är hans yrkesroll vilken information har han tillträde till i sin yrkesroll? Nästa steg är vilken information vill killen hantera? Är den öppen känslig eller intern? Nästa steg är vilken enhet vill han hantera informationen på och hur kan han skydda den? Är det en laptop, stationär dator, mobiltelefon eller vad handlar det om?

Och man kan besvara dem frågorna och ta ställning till säkerheten på dem nivåerna så att säga så kan man egentligen hantera vilken situation som helst så jag tycker det är en rätt bra tumregel.

Ok, så man skall ifrån varje fall så att säga anpassa säkerheten utefter vad som är behovet så man skall inte ha någon helhetssyn som man använder slaviskt.
Om man till exempel det här med vem tar vilken information på vilken enhet. Så om det kommer en säljare till exempel och köpt en ny Nokia Communicator som han vill använda för att komma åt e-posten. Då mappar man det mot den här frågeställningen, vem är personen? Vilken information vill han hålla på med? Och vilken enhet vill han ha det på? Och om vi inte kan skydda Communicatorn eftersom vi inte har köpt några licenser så faller det ju redan där. Då får man inte komma åt e-posten eftersom vi inte kan skydda den. Om man mappar frågan mot det verkliga livet så blir det mycket enklare. Om samma säljare med en laptop som har filkryptering och flera lager skydd på då är det ok va, under förutsättningar att han får komma åt sin e-post normalt sätt och det får han väl?

Vi har ju ökat Internet användningen ganska drastiskt bland företag och privatpersoner vilka medför ökat Internet användande enligt dig?
Målbilden ökar ju för elakingarna, om vi antar att det är 10% av populationen på Internet som är benägna att klicka på sidor och gå på bedrägerier. Så kommer ju ett ökat antal ändvändare av Internet bli ett ökat antal personer som går på de här bedrägerierna, vilket ger elakingarna en större målgrupp så att säga, man tjänar mer pengar på det man gör. Så att riskerna är ju det antalet användare som ger sig ut i det stora blå.

Ok, med elakingarna menar du?
Hackare, virusskrivare, bedragare och sådana saker.

Hur kan man öka användarnas säkerhetsmedvetenhet på ett bra sätt tror du?
Det här är ju den konstanta käpphästen, utbildningsbehovet är ju enormt samtidigt som det är ett ganska stort motstånd från att lära sig sådana här saker. IT-säkerhet och att tänka efter före och inte klicka här och ladda ner sådana här filer och skicka roliga saker till varandra allt sånt där är ju liksom party pooper. Den som kommer med regler och riktlinjer och förbud och sådant där, han ramlar ju av allas julklappslistor till slut. Så att jobba med IT-säkerhet ute på företag är ju då väldigt otacksamt. Man har pamfletter när man skriver enkla regler man kanske tar fram PowerPoint slides eller man spelar in videofilmer med personalen bara för att visa på olika scenarier som man kan stöta på och hur man kan hantera dem. Samtidigt som personalen sitter o tänker på vad de skall handla till helgen och vad de har sett på tv igår, man är inte alls intresserad då. Så det gäller att göra det lättförståeligt för personalen man pratar deras språk och framför allt då att man inte bara förbjuder och låser ner utan förklara varför man gör det. För det är väldigt lätt som sagt att bli hatad av alla när man jobbar med IT-säkerhet. Men om man förklarar med personalen eller personerna man pratar med varför man inte skall klicka på allting som kommer in i e-posten eller varför man inte skall ladda ner porr på företagets datorer så får man dem på ett annat spår. Och det viktigaste av allt är att skapa vi känslan att det är vi som skyddar vårt företag mot elakt ute på Internet istället för att komma med pekpinnen och säga du får inte ladda ner det och du får inte klicka där.

Vad tror du om sådana lösningar som går ut på att man ger användarna begränsade rättigheter?
Det är absolut jättebra, man skall inte ha ett dugg fler rättigheter än vad man absolut behöver. Inte ens administratörer bör sitta som administratörer hela tiden, utan man bör logga på som administratör när man skall göra administrativa saker och sen skall man logga på som vanlig användare igen, tycker jag. Men samtidigt förstår man ju att det blir som det blir i ute

verkligheten. Eftersom man inte ens kan ställa in klockan om man inte är lokal administratör så IT-personalen får ju väldigt många förfrågningar hela tiden som härrör till att man har begränsade rättigheter så det är både för och nackdelar. Man skall generellt sätt inte ha mer rättigheter än vad man absolut behöver i sin yrkesroll. Det är därför det heter administrativa rättigheter för att administratören skall ha dem, när han gör administrativa saker.

Om man hårdrar det så är det egentligen människan som är slarvig som utgör de största riskerna eller problem så att säga när det gäller Internetrelaterade hot.
Om man analyserar de incidenter som händer på ett företag. Så ser man någonstans 70-80% av incidenter är orsakade av felaktiga konfigurationer eller att man har fel rättigheter och sådana saker. Efter det kommer dåliga uppdateringar det kommer elak kod och sådana här saker och sen insiderbrott och sist av allt kommer stulna datorer. Så felkonfigureringar och för mycket rättigheter och sådant där står för absolut flest incidenter som finns. Till exempel att man har glömt att stänga av mail relay på mailservern eller att nånting har hänt på webben som tillåter att man hackar en, så det mänskliga slarvet är ju det som orsakar flest incidenter och sen det som är allvarligast det är en annan sak.

Du pratade innan om uppdatera programvaror, patchningar och sådana grejer. Är det organisationen då som skall denna se till att ha uppdaterat vad är det centrala.
Det här är alltså ett problem för organisationer som ökar enormt och det flera rötter till problemet som ger flera olika typer av problem. Ett av problemen är för organisationen är att hinna uppdatera sig om vilka nya sårbarheter som dyker upp, vad de innebär och vad man kan göra åt dem. Idag dyker alltså i snitt upp ungefär 10 nya sårbarheter om dan om man räknar in alla operativsystem och applikationer som finns. Har man en standardiserad miljö med XP-klienter och med Windows 2003 server så har du ganska få av de här sårbarheterna som berör dig, eller så ser inte verkligheten ut. Varje ny applikation som installeras på produkterna och enheterna medför en ökad risk för nya sårbarheter. Och vet då inte IT-avdelningen om vilka applikationer som finns installerade på de olika klienterna ute på nätverket, då kan man inte reagera ens om man ser att det finns en sårbarhet i winamp eller vad det nu kan vara om man inte vet att winamp är installerat på klienterna i nätverket. Så ett av problemen man har idag är att man inte vet vad som installerat därute eftersom man inte har låst plattformen tillräckligt. Nästa steg är ju då att få reda på rätt information om sårbarheten. Vad innebär den vad får den för följd finns det hackingverktyg därute var finns patcharna hur ser jag att patchen är rätt genomförd. Steget efter det är att hitta patchen testa den i nätverket och sen uppdatera klienterna. Sen har du ju nästa steg i problematiken folk envisas med att ha semester och vara sjuka, mammalediga och ute på resa och sådant där. Man måste få tag i alla burkarna för att kunna uppdatera dem. Och till dess att du vet och har på papper i princip att varje dator har patchen installerad och är verifierad att den är installerad och klar, så måste du anse att du är osäker. Och dyker det då upp tio nya sårbarhetslarm plus uppdateringar till varje om dagen så kan man inse vilket stort problem man har därute. Ju större företag man har desto dyrare blir det att göra de här patchhanteringarna. Många av systemen som man måste uppdatera kan ju heller inte tas ur bruk eftersom man måste vara online hela tiden. Så det är en väldigt tricky situation. Problemet är att patchhantering måste fungera. Men eftersom det dyker upp så många sårbarheter hela tiden, man hinner inte patcha mot allting man tvingas att välja och det gäller att då veta vilka sårbarheter man skall reagera först och snabbast mot. Det gör ju då att patchhantering måste fungera och ligga i bakgrunden och bara tugga på men samtidigt kan man ju inte förlita sig på det som skyddsmekanism utan det måste finnas där som ett såkallat skyddsnät. Ifall man tappar fotfästet eller ifall man råkar ut för någonting så skall patchhanteringen finnas där i bakgrunden för att täppa upp de här säkerhetshålen så man slipper trampa snett. Utan åter igen man måste bygga upp lager på lager av säkerhet utanpå den här osäkra kärnan, det här säkerhetshålet. Som gör då att ingenting kommer åt och kan utnyttja säkerhetshålet.

Om du tänker dig att du har något säkerhetshål i en webbläsare och en anställd surfar in på en sida som är preparerad med en exploit som utnyttjar säkerhetshålet för att ladda ner och exekvera kod på din dator. Har du då t.ex. ett antivirusprogram så kan den förhoppningsvis känna igen koden som kommer dansande. Har du ett intrångsdetekteringssystem så kan den känna igen själva exploitkoden när den kommer från webbsidan och har du en personlig brandvägg så kommer den att larma när det nya programmet som eventuellt har installerats kommer att försöka kontakta Internet. Så att man har det här lager på lager med skydd som skyddar den osäkra kärnan. Det är så det måste fungera idag.

Många standarder påpekar hela tiden att det är viktigt i företag att man skall ha ett incidentrapporteringssystem. För att vara beredd på nya problem det kan vara kopplat till att de ser någon användare som slarvar med någon policy alltså någon form av storebrorsövervakningssystem kanske. Eller det kan bara vara det att de är rädda att de har fått något virus men inte vågar erkänna det eller någonting sådant. Tror du att rutiner för incidentrapportering kan hjälpa och öka medvetandet hos de anställda?
Det är väldigt viktigt att IT-avdelningen får reda på vad som händer. Jag hörde ett skräckexempel för några år sedan där det var en IT-säkerhetschef som avskedade eller fick en person avskedad eftersom han råkade infektera företaget med virus. Och personen hade då endast klickat på en fil bifogat med e-posten. Och sen anmält det då, ”oj jag gjorde fel förlåt mig” och sen blev han avskedad för det. Vad som händer då är att ingen nånsin kommer erkänna någonting hädanefter och då sitter man där på IT-avdelningen och vet inte vad som händer ute i organisationen. Så det är viktigt att man skapar just en atmosfär som uppmuntrar till att folk rapporterar märkliga saker. Och framförallt till exempel support avdelningen eller IT-avdelningen är ju de som absolut måste ha öronen öppna för är det några som får in några förfrågningar om märkligheter i nätverket så är det ju supportavdelningen och IT-avdelningen. Man kanske rapporterar in att man har sett några konstiga ikoner eller datorn uppför sig märkligt här och var. Så det är oerhört viktigt att man får ut det i själva arbetsmiljön på företaget att man är villig att rapportera in saker. Och sen att man kanske får en klapp på axeln som tack för hjälpen efteråt. Så att man som företag vidtar rätt åtgärder för att uppmuntra den här typen av beteende för det värsta som kan hända är att man straffas för ett oriktigt beteende fast än man egentligen ville väl eller man gjorde någonting av misstag eller man gick på en luring som var väldigt snyggt uppsatt. Utan om man börjar med sådana typer av bestraffningar då sitter man snart och famlar i mörkret.

Vad har användarna för eget ansvar enligt dig?
Användarnas ansvar är att läsa och förstå vilka policys och regler och riktlinjer som är uppsatta av organisationen de måste förstå att den datorn som de har fått tilldelad är ett arbetsredskap och inte sin privata leksak. Man skall inte låna ut den eller föra över en massa konstiga filer och göra saker som inte är direkt arbetsrelaterade. Vad det gäller mobiltelefoner om vi skall återgå till mobilitetsproblemet. Så är det här ett jätteproblem för företag för att många anställda använder sina privata telefoner i tjänsten. Man kanske har fått någonting i födelsedagspresent eller köpt själv eller vunnit den i någon tävling. Och så tar man den till jobbet och trycker in den och börjar synka saker. Och då kan inte företaget påverka telefonen alltså installera saker eller ändra inställningar eftersom det är hans privata telefon. Så det enda som återstår då är att förbjuda honom att använda den i systemet. Men nu spårar det över lite från din ursprungliga fråga *skratt*. Men de anställda måste förstå vilka regler och riktlinjer som finns i företaget, så det är egentligen företaget som har det största ansvaret att se till att de anställda har läst och förstått policyn, inte bara läst den. Så du har ju tre steg, dels är så att man läser en policy, dels att man läser och förstår en policy och det tredje och viktigaste att man läser, förstår och utför det som står i policyn.

Och många företag saknar idag funktioner för att kontrollera förståelsen ute hos de anställda man kanske har kommunicerat ut nya regler och riktlinjer men man har inga verktyg för att få rapporter tillbaka som visar på vilken grad av förståelse man har för dessa regler och riktlinjer. Och sen någonting som är viktigt också är det står i policyn hur man kommer att hantera incidenter som har hänt om någon har brutit mot någon regel vad inbär det. Man måste tala om då att det här kan komma att betraktas som en incident och så vidare. För om man inte talar om att det här kan medföra en bestraffning på ett eller annat sätt så har man ingenting att komma med sen ifall någon uppför sig illa. Om man inte talar om att, vi betraktar det här som en allvarlig händelse så de anställda hävda andra saker så kanske man har problem med folk som uppför sig illa.

Så företag är generellt sätt dåliga då på att utbilda och ha en aktiv roll när det gäller informationssäkerhet i sitt företag.
Ja man kanske har skrivit en policy eller någonting sådant där som man kanske till och med gett till de nyanställda men sen har man kanske inte gjort uppföljningar man kontrollerar inte förståelsen sen i vissa fall ser man också att policyn kanske inte är förankrad i verksamheten. Någon har suttit på sin kammare och skrivit en jättefin policy enligt en massa böcker och best practices och sånt där. Men man har ju inte pratat med organisationen, varje ny funktion eller säkerhetsinställning som man gör kommer ju påverka alla andras sätt att arbeta. Om man inte har fått feedback och frågat de andra i organisationen om vad de tycker och sen korrigerat ramen efter det så kan man ju få problem sen med verksamheten. Man måste komma ihåg det att det är IT-säkerheten som är verksamhetsstyrd, det är verksamheten som har mål och visioner som IT-säkerheten skall stödja, inte tvärtom. Till exempel om du har ett supportcentrum eller kundtjänst eller någonting sådant där och sen drar du på en ny säkerhetsfunktion som gör att varje ny sida som visas för kundtjänstanställda tar 10-15 sekunder längre att visa på skärmen och sen är det 100 personer som skall ta 100 samtal per dag så de här 10-15 sekunderarna blir snabbt väldigt mycket arbetstid. Så att om man inte får in feedbacken utifrån organisationen så kan man räkna med att stöta på patrull.

Hur har mobiltelefoner förändrat säkerhetsproblemetik den senaste tiden?
Mobiliteten ökar, vi vill ju röra oss och koppla upp oss överallt och hela tiden. Många företag har ju uttryckligen sagt att våra anställda skall kunna sig överallt och hela tiden och skall kunna komma åt informationen överallt och hela tiden. Så man vill alltså ha maximal upptid och tillänglighet, men mobiltelefoner och den mobila världen kommer vi allt närmare det målet. Det gör ju också det att man måste sätta säkerhetsreglerna efter det. Vi kommer inte bli mindre mobila framöver.

Vilka är riskerna idag, hur stor är hotbilden mot telefoner?
Det största problemet är du glömmer den eller tappar den eller blir bestulen på den, det är det absolut största problemet idag. Och har du då inte kryptering så har du allting ute. Sen så börjar det komma problem i form av elak kod alltså virus och trojaner och viss mål även maskar som infekterar mobiltelefoner och sen sprider sig vidare via till exempel bluetooth eller MMS. Det är synd att säga att det är problem idag men det är på väg att bli ett problem det gäller att redan idag förbereda för att det kan komma någonting stort som kan sprida sig snabbt, förstöra mobilen eller stjäla information eller någonting sådant där. Det finns en 150 kanske olika virus, maskar och trojaner idag för mobiltelefoner främst Nokia Symbian telefoner. Vad gäller hackingattacker och intrång och sådant där så måste man komma ihåg när man är ute och surfar med 3G och sånt där så är du på samma Internet som alla andra i hela världen är och din telefon har en IP-adress, det gör ju att den är hackbar i princip.

Finns det brandväggar i mobiltelefoner.

Ja vissa modeller vissa, vi har ju till exempel till Nokia c60.

Ok som Symatec som levererar då eller?
Vi har det, jag har det i min mobiltelefon.

Hot ifrån Internet-relaterade faror. Är de ett stort hot mot driftsäkerheten och till exempel uptime i företag idag?
Om man tittar på hotbilden generellt sätt det senaste året så har den vridits från ”hacking for fame” alltså man vill ära berömmelse för det man gör till ”hacking for fortune” att elakingarna satsar allt mer på att försöka tjäna pengar på det de gör. Vad det gäller hot mot drift och uptime och sådant så använder man idag väldigt ofta så kallade botnet alltså zombienätverk alltså man har installerat fjärrstyrningstrojaner på bredbandsanslutna hemdatorer och så vidare som man använder i koordinerade attacker mot vissa webbplatser sen använder man det så för klassisk utpressning så att man kör igång en sådan attack mot ett företag och sen kontaktar man dem och säger det är var illa det här var väl otrevligt, betala oss 10 000 euro på det här kontot så försvinner problemet. Alltså det här klassiska beskyddar scenariot. Under 2005 så såg vi nästan 256 000 sådana här attacker, ungefär 1400 om dagen. Så att det sköt verkligen fart förra nyår det var nästan precis som någon startat upp ett företag som kommersiellt gör den här typen av attacken. Så det är väldigt omfattande.

Du sa innan att det är jäkligt viktigt att se till att uppdatera viktiga programvaror. I vissa studier så är företag rädda för att uppdatera nya versioner av program även om det kan innehålla fixar, för att de är rädda att det skall komma nya buggar de är inte säkra på att de skall fungera. Bidrar det till att företag är dåliga på att uppdatera? Slarvar de även med att uppdatera antivirus också på grund av sådana här grejer?
Nej inte själva virusdefinitionen men själva applikationen alltså själva antivirusprogrammet. Definitionerna kanske man automatiskt varje dag eller flera gånger per dag men själva programmet kanske man kan släpa efter lite med. I vissa fall sitter man ju fast i sådana här outsourcing avtal med andra företag vars uppgift är att uppdatera och så vidare så att man kanske inte ens kan uppdatera sin programvara för att man i princip inte äger sina maskiner utan det är outsourcing partnern som skall göra det åt en. Men du har rätt det är många företag som släpar efter en eller flera versioner en del gör det med flit också att de antar att nya versioner har nya problem man vet att den gamla funkar att patcharna har redan kommit och man har upptäckt de flesta säkerhetshålen och man väljer att inte ligga i tekniska framkanten och det finns ju fördelar med det då. Nackdelen är ju att nya versioner kanske innehåller bättre säkerhet än vad som fanns i dem gamla även fast man har patchat dem och säkrat upp dem. Så det där måste man nästan avgöra från fall till fall men helt klart är det att det kostar enorma summor för stora företag att uppgradera till nya versioner. Så det gäller att testa dem ordentligt och utvärdera dem och se hur de kommer att ändra nätverket ute i nätverket.

Så skall de försöka skilja på en säkerhetsuppdatering och en funktionsuppdatering?
Ta Skanska till exempel, Thomas Caser där han sa att det kostar ungefär en miljon för dem att skicka ut en ny patch i organisationen och då förstår man att de inte gör det varje dag.

Ja! Varför tror du att informationssäkerhet är ett så pass komplext problem?
Det är ett komplext område, det låter väldigt enkelt skydda informationen men det finns så många olika typer av hot allt ifrån brand och rök och folk som stjäl hårdvara till folk som klickar fel knapparna och raderar fel fil på servern till hacker attacker och elak kod. Och det gäller ju att täcka upp allting. Vi var inne litegrann innan på trådlösa nätverk mot trådbundna nätverk en del företag har ju problem med att veta om de är så att de har trådlösa nätverk för det kanske är någon på säljavdelningen som har satt in det i ett konferensrum för att slippa sladdar. Andra

delen för trådbundna nätverk kanske inte vet var alla nätverksuttag finns och om det går det skyddade eller oskyddade nätverksdelar. Så det är omfattande problem som berör allt ifrån den fysiska säkerheten till den mest högkrävande attackscenariot till glömska, slarv, sabotage och så "the force mayor" *skratt*.

Jordbävningar?
Ja precis eller blixtrat o sånt där.

Har du själv blivit drabbad av illvillig kod?
Nej inte virus maskar och trojaner däremot har jag varit av med mitt kreditkortsnummer förra året, vet inte varför eller hur.

Du skall inte surfa på så konstiga sidor.
skratt Jag tror att det var någon taxi eller restaurang eller någonting som drog det två gånger.

Det är märkligt att folk inte är rädda att ge sitt kreditkort till en liten 16-åring på Mc Donalds men är rädda för att ge ut det på Internet.
Precis

Dina bästa tips till en användare och en säkerhetsansvarig när det gäller just mobilitet, säkerhet, illvillig kod och sådana grejer.
Jag skulle generellt sätt vilja skilja laptops och mobiltelefoner när man pratar (oklart vad han säger) gå ihop till samma för det finns ingen skillnad just idag så vad gäller laptops så är det här med lager på lager med säkerhet som täcker upp varandra, man måste skydda datat de datat som lagras hanteras och överförs. Till exempel att på en laptop så kör man personlig brandvägg, antivirus, IDS och filkryptering eller diskkryptering plus VPN-koppling när man kopplar upp sig mot företaget. Vad det gäller mobiltelefoner och sådana saker så måste man hålla kontroll på den nya tekniken som kommer ut, man måste köra standardiserade plattformar om man skall tillåta informationshantering, Alltså företagets information på dem här enheterna. Och man måste se till att man kan skydda de enheterna som vill användas och sen våga säga ifrån. Att vi kan tyvärr inte skydda den här enheten det innebär att du inte får hantera e-post eller företagskänslig information på den här enheten. Så att det bästa tipset det är att i policyn specificera vad som gäller för varje enhet.

Hur kan företag kontrollera vilken information som finns på enheterna?
Det kan man inte.

Det finns inget sätt idag?
Nä, det finns ju loggar och sådant där som man kan se vilken information som vilken person har kopierat eller sånt. Men det är oerhört svårt.

Vilka produkter eller tjänster får ni (Symantec) mest förfrågningar om från företag.
Vi gick ihop med Veritas så jag kan inte riktigt hela deras produkt utbud. Men vad säkerhetssidan så har vi den här "mantec client security" som just den här typen av lösning där man har flera olika säkerhetsprogram som täcker upp för varandra. Som antivirus, personlig brandvägg och en enkel IDS. Folk har förstått att ett vanligt antivirus program inte räcker idag och vi säljer ju också förhållandevis lite av rena antivirus program utan det är just det hära client security för hemanvändare som är motsvarigheten Notron Internet Securtity där man har flera olika säkerhetsprogram i samma skal. Vidare på företagen har vi väldigt mycket backupprogramvara som backupexec som har funnits i alla år vi har också olika typer av programvara för att snabbt kunna återställa system om något har brunnit eller gått ner eller någonting sådant där. Också olika

typer av patchhanterings system att man snabbt och enkelt kan se vilken dator som saknar vilken patch och sen trycka ut den till den maskinen. Så om man säger att man har varit på semester eller pappaledig eller någonting sådant där och kommer tillbaka med sin laptop och pluggar in den så känner systemet av automatiskt att här saknas det vissa patchar och fixar den problemet.

Just det här med att kunna återställa systemen, har det också förändrats i och med att det har gått mer och mer emot lättborttappade enheter?
Ja och nej, man tycker ju då att det dyraste vid ett inbrott det tycker man ju är laptopen eftersom det kostar en massa pengar att köpa nytt, men det dyraste vid ett inbrott när man blir av med en massa datorer är ju informationen som ligger på. Försäkringen kommer att täcka upp att få en ny enhet, mobiltelefon, laptop eller vad det nu kan vara. Men om du inte vet vilken information som fanns på enheten du har ingen bra backup och så vidare så tar det jättelång tid att återställa och att se till att den anställda kan börja arbeta igen och bli produktiv, plus att du inte vet vilken information som finns ute i vida världen. Har du backuper som är bra tagna med korta intervall så kan du snabbt bara stoppa in ny hårdvara lägga tillbaka backupen sen är personen igång igen plus att du vet vilken information som fanns på datorn ungefär när den blev stulen eller förstörd. Så backup tagning och återställningssystem är oerhört viktigt idag för att egentligen spara pengar. Och dem lösningar blir smartare och smartare ju längre tiden går.

Och backuper och sådant skall då förvaras off-site så att säga?
Ja gärna både och så att du har snabba backuper till exempel med snapshots som tar inkrementella backuper imellan dem stora fulldisk backuperna och sen portar du dem vidare då till billigare backuplösnigar som tejper och sånt där som du sen skeppar off site. De måste finnas på något annat ställe ifall det värsta händer.

Har du hört talas om BITS från krisberedskapsmyndigheten?
Har bara läst deras lathund inte läst något mer.

Ok det är ju mer generella riktlinjer för organisationer och företag för att uppnå absolut minsta basnivå. Tror du att företag är i behov av det?
Allting man kan göra för att lätta upp för de här stackarna kommer ju att underlätta att det tas emot varmt ute på organisationerna. Problemet är att de ger bara minsta basnivå på säkerheten men om man skall gå ner lira lite grann på mer finområden så då står man fortfarande där och vet inte hur man skall bete sig. Det finns jättemånga bra riktlinjer hur man sätter upp antivirusprogram eller en brandvägg men om man kommer ner på andra typer av IT-säkerhet så är det fortfarande väldigt svårt.

Det är där konsulter kommer in eller?
Typ *skratt*

Du skall ha ett stort tack!
Det är helt ok alltså, jag hoppas att du får ut något av det.

Bilaga 5, Expertintervju Johan Jarl, F-Secure

Kort presentation om bakgrunden till intervjun.

Hej Johan, kan du berätta lite om din bakgrund och arbetsuppgifter?
Hej, jag har jobbat med IT-säkerhet sedan 1999, då jag började jobba på Protect Data numera PointSec, med då autentiseringslösningar, VPN, PKI och sådana saker. Sen 2002 började jag på F-Secure där jag är tekniskt ansvarig över verksamheten i Sverige. Det är allt som har med teknik och säkerhet att göra egentligen.

Vi kommer att gå igenom lite frågeområden vi får se hur många vi hinner med pg. av din tidsbrist. Om vi börjar med mobilitet. Hur har säkerhetsbehoven för företagen ökat i och med ett ökande användande av mobila enheter? Att mer mobil hårdvara har tagits in i organisationerna?
Det är klart, tar man in hårdvara för att göra företagen mer och mer mobila, för att affärsverksamheten ska bli mer flexibel, det innebär att man får in helt annan säkerhetsproblematik då. Folk som har sina datorer hemma kopplar upp sig, så kraven på säkerhet har ökat, absolut. Just på grund av att man har mobila plattformar

Ok, när man kopplar upp sig utifrån vad medför det för risker för företaget?
Risken finns ju att man får in något skräp på sin dator när man surfar via sitt hemmabredband, sen blir det en språngbräda rätt in i företaget via då exempelvis VPN, då man har en direktuppkoppling mot företaget. Det andra sättet är ju att man har sin dator hemma, får in något skräp på den och tar sedan in den bärbara datorn på företaget, då spelar det ingen roll hur stor och fin brandvägg företaget har. Man bär in problemet direkt in på företaget. Det är det vanligaste. Vissa företag, de flesta företag som har blivit drabbade av nätverksmaskar har ju fått det just genom att anställda burit in masken på sina bärbara datorer

Så man går igenom företagets perimeterskydd så att säga?
Ja precis, genom att ta med sig en bärbar dator in på kontoret, som har blivit smittat hemma. Ett annat alternativ är att en barn till exempel använder den anställdes dator för att fildela eller någonting, och får in skräp den vägen också. Det finns ju många olika vägar att få in skräpet då.

Ok, vad har företagen för verktyg, eller metoder kanske man kan säga för att skydda sig mot just det här att perimeterskyddet brister?
Ja det är så här att, självklart ska det finnas policys, ett regelverk för hur man ska använda sin bärbara dator. Samt att man har ett antivirusprogram såklart, en personlig brandvägg på datorn. Sen så klart, det är då det största skyddet man har egentligen. Att man har en brandvägg och ett antivirussystem på den bärbara datorn samt ett regelverk som de anställda får följa.

Och uppdaterad mjukvara då eller?
Ja precis, absolut.

Ok, tack. Vilka mobila enheter enligt dig medför mest risker idag?
Det är ju fortfarande en bärbar dator helt enkelt, det är fortfarande största hotet. En mobiltelefon är inte ett stort hot ännu även om det är ett växande problem. Det finns ju andra mobila

lösningar såsom USB-minnen och sådana saker. Man lagrar offerter eller vad det nu kan vara, man tar med sig det hem, det blir en genväg att kunna lagra information på exempelvis MP3-spelare som nuförtiden har hårddiskar, där man inte har någon kryptering som man då kanske har på sin bärbara dator. Men det största problemet är en vanlig bärbar dator helt enkelt.

Det här med att om en mobil enhet blir borttappad eller stulen, kryptering är ju en teknik då för att skydda informationen så den inte kommer i fel händer, används det mycket idag? Är företagen medvetna om att de kanske behöver kryptera viss information?
Jag tror inte det, jag tror inte att de flesta är det, jag har ingen procentsatts på det men jag tror inte det är speciellt jättemånga som använder kryptering. För det är lite krångligt, och ja visst det stjäl lite prestanda och så vidare. Men jag tror inte det är så jättevanligt att man krypterar informationen på sin dator. Blir ett företag av med en dator tror jag inte att de har krypterat informationen, oftast.

Och det kanske är ännu mindre på mobila enheter som PDA och mobiltelefoner då eller?
Ja precis, den är väldigt minimal den krypteringen hos företag som använder PDA och sådant. De stora företagen har tagit grepp kring mobiltelefoni och handdatorer, de har ju fixat ett krypteringsprogram så klart, men det finns ju många som inte har det.

Tror du ett av problemen är att företagen inte vet vilken information som ska krypteras? Att just informationsklassificering är ett problem, tidskrävande och det finns ingen automatisering för det, eller vad man ska säga?
Nej det tror jag inte är ett problem, som hårddisk..Det finns ju många olika typer av kryptering, hårddiskkryptering tillexempel det svenska företaget PointSec, eller Protect Data där jag jobbade tidigare har, då krypterar man ju hela hårddisken. Oavsett vilken information man har kommer allting att krypteras, så nej det tror jag inte är ett problem.

Ok, tack! Med mobilitet kommer ju trender såsom distansarbete, och att folk vill vara just mobila bidrar ju till tekniker så som då WLAN. Vad medför WLAN för risker?
WLAN så klart det innebär ju en risk, men så klart har du den bärbara datorn hemma och du använder trådlöst nätverk, om den bärbara datorn har en personlig brandvägg som är rätt konfigurerad så medför ju det inget problem. Om trafiken dessutom är krypterad via VPN så är det inget problem alls. Däremot kan ju någon annan kanske använda det trådlösa nätverket för att göra någonting dumt så att personen som har bredbandet kan få skit för att han har skickat ett spam eller vad det nu kan vara. Men den själva bärbara jobbdatorn ser jag inte som ett problem, om den är korrekt skyddad.

Inom företaget då, om de använder ett trådlöst nätverk för att de ska kunna ha kanske Internetanslutning i ett konferensrum eller något annat. Medför det hot, eller en ny form av problematik?
Ja det medför det. Det är ett jätteproblem, jag vet många företag där en anställd har tagit med en basstation och sedan stoppat in den i företagets nätverk. För att de ska kunna arbeta smidigare. Det är ett riktigt stort säkerhetsproblem, men självklart om installationen av basstationen sker på ett korrekt sätt på ett företag så ser jag inga problem med det. Problemet är att gör man det på korrekt sätt, så att det ska vara helt säkert. Då är det inte så mobilt längre, det är då inte så enkelt att använda det. För att det blir ganska jobbigt att använda det, då går man bort från det här med smidigheten med mobilitet, det blir bara krångligt att använda det istället. Det är då att man sätter en basstation och kopplar in den på Internet, brandvägg emellan och man har autentisering och så vidare. Och man tillåter bara VPN-trafik genom brandväggen, det blir som distansarbete egentligen, fast på kontoret då.

Ok
För att trådlösa nätverk ska man se som ett Internet egentligen.

Är du av uppfattningen att företag är medvetna om riskerna med just WLAN? Wardriwing och den typen av hot.
Ja det tror jag, företagen är nog medvetna om det. Men däremot finns det säkert anställda på företagen som installerar det på eget bevåg. Problematiken är ju däremot mycket större hos hemanvändare, som inte känner till det knappt. Det går till On-Off och köper en trådlös router och installerar den och så fungerar det, sen struntar de i det. Det är lite pilligt om man inte är datorintresserad att hålla på med krypteringsnycklar och sådant. Hos hemanvändare är det då ett stort problem, hos företagen inte ett så stort problem. Förutom att just användare på företaget tar då med sina egna basstationer och kopplar in.

Ok, tack. Om vi hoppar lite till drifthantering eller vad man kan säga, om man tappar bort en mobil enhet kan ju återställning vara centralt för att personen ska kunna komma igång med sitt arbetet snabbt .Vad är dina tankar om det?
Säkerhetskopiering är det nog sämre med ute på företagen, man skyddar informationen på filservern och så vidare. Men det är inte jättemånga som har rutiner och sådant för att kunna återskapa en dator, framförallt inte en mobil enhet. Speciellt inte handdatorer och sådana saker, även om det finns verktyg gör det möjligt. Men jag tror inte att det är jättemånga som gör det. Utan man fokuserar mer på servrarna på företaget.

Ok, tack. Vi hoppar till personalrelaterade frågor.
Mm

Vi har fått indikationer på att företag ska utbilda personalen för att få ett ökat medvetande när det då kommer till informationssäkerhet. Hur utbildar och informerar företag sin personal för att arbeta på ett säkert sätt?
Man ska ha regelbundna möten med personalen och informera dem om hur de ska arbeta med sin dator. Man ska ha en lätt säkerhetspolicy, en säkerhetspolicy ska inte vara ett jättestort dokument, utan den ska finnas på ett papper som vem som helst kan läsa och förstå. Det ska finnas lättillgängligt. Det är ett problem idag tror jag, att man gör en säkerhetspolicy som är väldigt lång och komplicerad, sen lägger man den i en hög och säger att ja vi har en säkerhetspolicy på företaget. Men det är då bättre att man har en liten, en förenklad säkerhetspolicy till den komplicerade och har den lättillgänglig för de anställda. Sen att man då utbildar de anställda i hur de ska följa den här policyn och då gå igenom nya hot och sådana saker som dyker upp.

Ok, slarvar företagen med att konfirmera att säkerhetspolicyn har tagits upp i organisationen?
Ja absolut, oftast är det ett dokument som ingen har läst, någonsin. Utan det är bara någon som har skrivit den och sen sagt att nu har vi en säkerhetspolicy. Men de har inte kontrollerat att någon har läst den eller förstått den. Möjligtvis har man skrivit under något papper, vid anställningen, men ingen som då har läst eller förstått de här policysarna , det tror jag inte.

Lösenordspolicys verkar ju vara rätt vanligt. Vad är dina synpunkter kring detta?
Det ska ju vara långt och komplext, självklart. Man pratar om att de ska ha fraser istället, det säkraste är ju kanske att ha en säkerhetsgenerator då egentligen, det är ju det enklaste. Men det blir ju…Ganska kostsamt att driva då. Man ska då vad säger man, ha 14 tecken, specialtecken, stora och små bokstäver och så vidare. Man får ju inte göra det för komplext heller för då skriver användarna upp det på en lapp och lägger det under tangentbordet, så man får ju. Det är en

balansgång. Tar man istället då lösenordsfraser, så det blir lättare att komma ihåg är det klart att det är ett bättre alternativ.

Ett vanligt strong password helt enkelt?
Ja jag tycker det är helt okej.

Ett annat problem som kanske ökar med mobilitet är datorer befinner sig på andra platser än de brukar. Normalt sätt kanske de andra på kontoret har koll på den när man lämnar den obevakad. Vad finns det för problem där om man lämnar sin arbetsstation och den är mobil, framför allt laptops då. Jag vet att många företag har automatisk skärmsläckare med lösenordsinloggning igen då.
Det finns ju produkter för att kunna lösa det här, att man måste ha ett kort i sin dator, Det är väll bankerna som har det så att personalen har smarta kort för att göra transaktionerna sen tar du ur det ur datorn så låser sig datorn, samma kort använder du då för att gå in i fikarummet så man har det alltid med sig. Det är ju en dyrsam lösning men det andra är ju självklart att man har en skärmsläckare som går igång efter en 10-15 minuter, återigen upp till användarna, går man ifrån arbetsstationen så skall man låsa.

Vad är användarnas eget ansvar enligt dig?
Bra fråga, användarnas eget ansvar är. Det är ju att följa säkerhetspolicyn de regelverken som finns i säkerhetspolicyn och allt vad det innebär, även att låsa datorn såklart.

En annan teknik är ju begränsade rättigheter till användare. Vad finns det för tekniska hjälpmedel och tekniker för att kunna förhindra användare från att installera vad som helst på sina arbetsstationer.
Om man ser på vår produkt som vi har då så har vi en brandväggsdel. Brandväggsdelen har en applikationskontroll och så fort ett program försöker ta sig ut på Internet eller ut på nätverket. Så kommer administratören få upp en fråga om att det här programmet försöker ta sig ut på Internet. Så det är administratören som sätter rättigheterna om det har programmet skall få gå ut på Internet eller inte. Vilket innebär då att användaren kan installera Kazaa men han kommer inte få gå ut på Internet eftersom det är administratören sätter stopp på den nivån då. Det är ett sätt att lösa det på.

Du pratade innan om den här lager på lager säkerheten för att förhindra att man bara har ett starkt perimeterskydd. Vad finns det för andra saker inom företagets interna nätverk än just lager på lager skydd i mobila enheter som kan hjälpa till att förhindra spridning av skadlig kod om det har kommit in i nätverket.
Alla möjliga skydd såklart, intrångsdetekteringssysem på bärbara datorn, brandvägg, antivirus, självklart någon antispamprodukt, krypteringsprodukt, kan vara fil kryptering eller hårddisk kryptering sen så klart finns det ju olika former av engångslösenordsgeneratorer eller smarta kort för att skydda datorn och inloggningar. VPN klienter skall ha en krypterad tunnel. Det är väl det på en bärbar dator som jag ser.

Ute i det övriga nätverket då?
Det är olika, när man ser på ett antivirusprogram då skyddar det e-post servern, att man skyddar webbtrafiken, all trafik skall genomsökas filtreras, man har små agenter som kontrollerar nättrafiken och letar efter konstiga mönster. Det finns ju otroligt många olika typer av säkerhetsprodukter för att kunna få den här lökmodellen som man säger, för att få flera olika typer av skydd.

Hur vanligt är det med segmentering av nätverken för att minska spridandet?

Det blir vanligare och vanligare men fortfarande finns det företag som inte har det och som jag har varit i kontakt med och haft problem just med nätmaskar till exempel har inte haft segmenterade nätverk. Men jag tror de flesta som bygger om nätverken nu de segmenterar upp det så mycket som möjligt.

Jag tänkte på patchhanteringen hos företagen för att de skall skydda sig. Vad har du för tankar om just patchhantering och hur företag använder det och vad finns det för problem med det?
Patchhanteringen blev egentligen aktuellt 2003 när det var blaster som kom till, nätmasken. Då blev det väl hett och hur man skall sköta patchningen. Jag tror att företagen har blivit ganska bra på patcha just operativsystemet. Men däremot så kanske inte finns någon bra modell för att patcha Winamp eller vad det nu kan vara, alltså när det inte gäller operativsystem. Samma sak gäller det egentligen även mobiltelefoner och handdatorer där finns det inget bra sätt att patcha där finns det ingen Windows Update på en mobiltelefon i dagsläget. Så att patchning för bärbara datorer, patcha operativsystem och nu även Officepaketet det är ju bra. Men patchningen av andra mjukvaror som webbläsare eller MP3-spelare eller vad det nu må vara, den är ju sämre.

Är webbläsare just ett problem då eftersom mycket skadlig kod sprids just genom webbläsare?
Ja absolut. Det är ju operativsystemet och webbläsaren som egentligen är prioritet ett att ha uppdaterat.

Vad är din syn på säkerhetsstandarder som till exempel ISO 17799?
Det är bra att det finns standarder som företag kan följa och nu har inte jag dykt ner i den standarden sådär jättemycket men det är bra att det finns regelverk som företagen kan följa.

Just ISO är väl väldigt komplext och tungrodd och det är otroligt kostsamt att implementera den så har krisberedskapsmyndigheten tagit fram riktlinjer för basnivå för informationssäkerhet. Som då är riktlinjer för minimal informationssäkerhet, det minsta som krävs helt enkelt. Har du hört talas om BITS?
Nej det har jag inte.

Om du får ge ett tips dels till en IT-ansvarig som jobbar med informationssäkerhet och en användare om informationssäkerhet. Vad är dem tipsen?
Om jag börjar med användaren då. Läs igenom vilken säkerhetspolicy man har på företagen just för att kontrollera så man inte bryter mot den. Det är inte bra att bryta sin egen säkerhetspolicy det kan man få sparken för. Du säger informationssäkerhet och det är ju väldigt brett, väldigt brett spår. Det klassiska är väl det att man inte skall dubbelklicka på konstiga filer i inkorgen helt enkelt, det är ett stort problem.

Att vara uppmärksamhet helt enkelt?
Uppmärksam, misstänksam det är väldigt viktigt tycker jag, att man tänker efter. Det finns ju otroligt många olika typer av hot. Vara uppmärksam och inte dubbelklicka på konstiga filer i e-posten och kanske inte klicka på alla roliga länkar som följer med i e-posten. Samt att följa upp och kolla vad företaget har för säkerhetsregler.

När det gäller för nätverkskillen då så, utbilda användarna och gör det inte så komplicerat gör det ganska enkelt, säkerhet behöver inte vara komplicerat. Gör man det enkelt så att användaren förstår det så kan användarna även lättare följa säkerhetspolicyn. Sen såklart som nätverkskille då om man jobbar med det måste man ha omvärldsbevakning att man hela tiden försöker se vilka nya hot som kommer, det kommer upp nya hot hela tiden som de kriminella använder då. Så det

gäller att ha omvärldsbevakning då. Man skall inte köpa någon dyr lösning och tro att det är lösningen på problemet. Från dag till dag kan allting förändras så att man måste hela tiden omvärldsbevaka och utbilda användarna.

Är säkerhetspolicy organisationen eller kanske då ledningens sätt att kanske öka säkerhetsmedvetandet hos anställda?
Ja säkerhetspolicyn som företagen gör är ju oftast komplex och innehåller många olika delar man skulle kunna sätta ihop den och göra den lite enklare, så att den blir väldigt lätt att ta till sig, så du får ut den till användarna så att de verkligen förstår den.

Har du själv blivit drabbad av skadlig kod?
Nej det har jag faktiskt inte men däremot har mina släktingar. Det har ju kommit in någonting men det har ju stoppats såklart på sin hem-PC så det har kommit in någonting men då har det kommit ett virusvarningsmeddelande och tagit bort det då. Men däremot med släktingar händer det ju ibland att man får åka och hjälpa.

Känner igen det där.
Men däremot så faktiskt fick jag ett mobiltvirus för två månader sen på tunnelbanan faktiskt. Jag hade ju antivirusprogram i mobiltelefonen då så jag stoppade det då men det var någon som försökte smitta min telefon då på karlaplan tror jag det var. Så det är i och för sig väldigt ovanligt att man får det men det finns faktiskt i Stockholm.

Varför tror du just att informationssäkerhet är ett så komplext problem?
Därför dem som gör säkerhetspolicyn gör den för komplicerad, man kan göra den ganska enkel man behöver inte göra det så svårt för sig. Sen är det ju såklart så kommer det en massa nya hot hela tiden så det tar ju väldigt mycket tid att kunna göra just den här omvärldsbevakningen och se att vi verkligen är säkra.

Är det ett problem att det inte är ett problem som enbart går att lösa med teknik eller enbart med policys och regelverk.
Nej absolut inte, tekniken är ju bara ett hjälpmedel, det är ju inte lösningen utan det är ju att verkligen förstå organisationen och hur man skall skydda sig och vad det kostar för företaget. Och att verkligen utbilda användarna. Tekniken hjälper ju bara till att få säkerhetspolicyn att fungera tillsammans med utbildning och så vidare. Jag tycker att man i vissa fall gör det för komplicerat. Gör man det för komplicerat till exempel att jag kräver krångliga lösenord, då händer det att användaren tar den lättaste vägen och skriver upp lösenordet på en post-it lapp, det finns många olika exempel på det där. Gör man ett för komplext till exempel att man har för dyra komplexa säkerhetslösningar fast det man skyddar på företaget är egentligen inte lika mycket värd vad säkerhetslösningen kostar. Så man verkligen gör den här balansen att man inte gör det för komplext för användaren så det försöker gå runt den.

Bilaga 6, Expertintervjuer kompletteringsfrågor

Magnus Lindkvist, Microsoft AB

Hur kan man förhindra utbrott av skadlig kod?
Att förhindra ett utbrott till 100% är svårt. I en stor organisation är chansen att det finns en opatchad dator eller en oförsiktigt användare ganska stor. Att segmentera nätverk är en vanlig metod som man använder om man har legacy system. Legacy i det här fallet skulle exempelvis kunna vara WindowsNT. Eftersom WindowsNT är mer än 10år gammalt så är det inte längre supportat av Microsoft, men trots detta finns det företag som fortfarande kör med NT i produktion.

Att köra med ett så gammalt system i produktion innebär vissa risker och kostnader. För att få ner riskerna då så kan man tex sätta sina äldre system på ett separat nätverk - men det är ingen bra lösning utan en tillfällig sådan.

Vad har ledningens för ansvar och skyldigheter att sätta upp en policy?
När det gäller ledning så har dom det ultimata ansvaret. En VD ansvarar för ett företag - om något händer är han/hon ytterst ansvarig. Det är dock ovanligt att en VD engagerar sig direkt i säkerhetsfrågor utan har oftast deligerat detta till tex CIO, CSO eller CISO.

Per Hellqvist, Symantec Nordic AB

Hur kan man förhindra utbrott av skadlig kod?
Krasst sett kan man inte det, men man kan begränsa möjligheterna att infekteras och skadeverkningen av en eventuell infektion. Detta genom att applicera lager på lager säkerhet och arbeta med kraftfulla verktyg för backup och återställning.

Ett alternativ är att dela upp organisationens nätverk i mindre enheter med hjälp av segmentering, för att se till att en attack endast drabbar en mindre del av nätverket. Fler saker?
Segmentering är mycket bra, men har hamnat lite i skymundan de senaste 7-8 åren. Fördelen med ett segmenterat nätverk är att man kan stänga av delar av nätverket för att rensa upp och begränsa spridningen av elak kod. Man kan även använda personliga brandväggar för att skydda de enskilda datorerna från varandra även internt i nätverket.

Vad har ledningens för ansvar och skyldigheter att sätta upp en policy?
Ledningen har ju ansvaret för organisationen. Med en säkerhetspolicy som är läst och förstådd och efterlevd fungerar organisationen bättre. Det ligger helt i de ansvarigas område att se till att organisationen flyter utan problem.

Vad är enligt dig en bra lösenordspolicy, strong password ?
Minst åtta tecken med minst ett specialtecken och minst ett numeriskt-tecken. Lösenordet skall bytas t ex var tredje månad och får inte vara samma som de t ex 5 föregående.

Vem bestämmer hur information ska klassificeras?

De som är ansvariga för informationen, t ex affärsområdesansvariga. I slutändan är det högsta ledningen. Klassificeringen specificeras i policydokumentet

Vad bör användare tänka på när de lämnar sin arbetsstation?
Att låsa skärmen med ctrl-alt-del. Att inte lämna framme papper som innehåller känslig eller intern information. En "clean desk"-policy är viktig. Att ställa undan lösa backup enheter, CD-skivor och annan lagringsmedia.

Hur ska ledningen se till att styra lösenordskrav?
Genom att specificera i företagets IT-säkerhetspolicy

Hur ska organisationen följa upp och lära sig av incidentrapporter, händelser?
Snabbt och effektivt. Direkt efter en händelse sätter man sig och tittar igenom vad som hänt, varför och hur man kan förhindra att det händer igen. Allt revirpinkeri och liknande lämnar man in i garderoben. Här gäller det att på ett öppet och ödmjukt sätt erkänna att något gått fel och ha viljan att rätta till det så att det inte händer igen. Lär man sig inte när något gått fel har man gjort ytterligare ett fel.

7 Referensförteckning

Arbaugh, W. A. (2001), Your 802.11 Wireless Network has No Clothes, Department of Computer Science, University of Maryland. College Park, Maryland, USA.

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

Ballou S., (2003) MALICIOUS CODE – WHAT SHOULD WE DO?. Tillgänglig på http://www.sans.org/rr/whitepapers/malicious/1290.php, [2006, Maj, 26]

Bergman F., Hagströmg C. (2005). Skydd av data på bärbara datorer, En kartläggning av olika lösningar för att förhindra att värdefull information blir stulen. Institutionen för data- och systemvetenskap. Stockholms universitet / Kungliga Tekniska Högskolan

Bin Munir A., (2001) Managing Desktop Security. Tillgänglig på http://www.sans.org/rr/whitepapers/basics/520.phpnedladdat 270506, [2006, Maj, 27]

Bryman, A., Bresnen, M., Beardsworth, A. & Keil, T. (1998). Qualitative Research and the Study of Leadership. Human Relations, vol 41, Nr. 1, ss. 13-30.

Boeckeler, M., C. (2004), Overview of Security Issues Facing Computer Users, SANS Institute 2004, Tillgänglig på http://www.sans.org/rr/whitepapers/awareness/1399.php [2006, April, 12]

Caveo (2003). Laptop Computer Security. Tillgänglig på http://www.caveo.com/images/Caveo.Laptop%20Computer%20Security.Whitepaper.pdf. [2006, Maj, 5]

Chris H., Michael P., Russ R., Frank T. (2004). WarDriving: Drive, Detect, Defend,A Guide to Wireless Security. Syngress, New York.

CSI (2006), CSI/FBI Computer Crime and Security Survey, Tillgänglig på Tillgänglig på http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf [2006, Mars, 12]

Danielson, J. (2002), Wireless Security: Blackberry by Research In Motion, SANS Institute 2002, Tillgänglig på http://www.sans.org/rr/whitepapers/pda/258.php [2006, April, 23]

Davidson Bo och Patel Runa (1994) Forskningsmetodikens grunder, Studentlitteratur: Lund.

Edge L., (2000) Spyware – Identification and Defense. Tillgänglig på http://www.sans.org/rr/whitepapers/privacy/688.php, [2006, Maj, 26]

Freeman, T., Mikkelsen, B., Bonde, A., Forti, S., Huda, M., Keller, B., Possing, S. (2003),

Gender Equality. Elanders Novum, Stockholm.

Gold, J. (2006), Compliance in the Mobile Enterprise,
Tillgänglig på http://www.sybase.com/detail?id=1040583, [2006, Maj, 14]

Hietala, J. (2004), Network Security- A Guide for Small and Mid-sized Businesses
Tillgänglig på http://www.sans.org/rr/whitepapers/basics/1539.php, [2006, April, 23]

Halvorsen, K. (1992) Samhällsvetenskaplig metod. Studentlitteratur, Lund.

Holme, M. & Solvang, B. (1997) Forskningsmetodik. Studentlitteratur, Lund.

Krisberedskapsmyndigheten (2006). Basnivå för informationssäkerhet (BITS) – rekommendationer, Tillgänglig på http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/KBMs%20publikationsserier/Rekommenderar/bits_rek_2006_1.pdf, [2006, Mars, 12]

Krisberedskapsmyndigheten (2006), Samhällets informationssäkerhet, Lägesbedömning 2006, Tillgänglig på http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Utredningar%20och%20remissvar/Utredningar-uppdrag/lagesbedomning_infosakerhet_%202006_slutlig.pdf, [2006, Mars, 12]

Krisberedskapsmyndigheten (2005), Beredskap mot skadlig kod. Tillgänglig på http://www.krisberedskapsmyndigheten.se/templates/Archive____5278.aspx, [2006, Mars, 12]

KBM:s stöd i arbetet med informationssäkerhet, Tillgänglig på http://www.krisberedskapsmyndigheten.se/templates/EntryPage____6709.aspx, [2006, Mars, 12]

Ledell, G. (1991) Gör en informationssäkerhetsstrategi, Stockholm, DF (Dataförening i Sverige)

Lenander, R. (1998) För säkerhets skull, Höganäs, Kommunlitteratur.

O'Dorisio D., (2003) Securing Wireless Networks for HIPAA Compliance.
Tillgänglig på http://www.sans.org/rr/whitepapers/awareness/1335.php, [2006, Maj, 16]

Patel, R. & Davidson, B. (1994) Forskningsmetodikens grunder - Att planera, genomföra och rapportera en undersökning. Studentlitteratur, Lund.

Pointsec (2004). News from Pointsec mobile technologies. News from Pointsec mobile technologies, 3,4, Pointsec Mobile Technologies AB. Tillgänglig på http://www.pointsec.com/_file/PMT1_04_web.pdf, [2006, Mars, 12]

Pointsec (2005). News from Pointsec mobile technologies. News from Pointsec mobile technologies, 3,2, Pointsec Mobile Technologies AB. Tillgänglig på http://www.pointsec.com/_file/PMT05_no1_Global_72dpi.pdf, [2006, Mars, 12]

Price, R. (2003), The PDA as a Threat Vector, SANS Institute,
Tillgänglig på http://www.sans.org/rr/whitepapers/pda/998.php [2006, April, 23]

Rosenberry, T. (2003), Protecting Your Corporate Network from Your Employee's Home Systems, Tillgänglig på http://www.sans.org/rr/whitepapers/policyissues/1314.php [2006, April, 23]

Schoeman, K., Serote, P. & Woroniuk, B.(2003) Reflection on Experiences of Evalutation

SIG Security (1997) Riktlinjer för god informationssäkerhet, Studentlitteratur, Lund.

SIS, Swedish Standards Institute (2002) Handbok i informationssäkerhetsarbete: baserad på standarden SS-SO/IEC 17799 och SS 62 77 99-2. Ledningssystem för informationssäkerhet. SIS förlag AB, Stockholm.

Statistiska centralbyrån, (2005) Företagens användning av datorer och Internet 2005, Tillgänglig på http://www.scb.se/statistik/_publikationer/IT0101_2005A01_BR _TKFT0503.pdf, [2006, Mars, 12]

Statskontoret (1997), Handbok i IT-Säkerhet Del I
Tillgänglig på http://www.statskontoret.se/upload/Publikationer/aldre/199729A.pdf [2006,April, 12]

Straub, K.R. (2003), Information Security Managing Risk with Defense in Depth, Tillgänglig på http://www.securitydocs.com/library/1525, [2006, Maj, 14]

Symantec (2006), Symantec Internet Security Threat Report, Trends for July 05–December 05 (Volume IX). Symantec.

TeliaSonera, TeliaSonera Trendspaning 2006, TeliaSonera,
Tillgänglig på
http://wpy.waymaker.net/client/waymaker1/WOLReleaseFile.aspx?id=207417&fn=wkr0003.pdf, [2006, April, 16]

Trend Micro (2005), Security for Mobila Devices: Protecting and Preserving Productivity, Trend Micro, Tillgänglig på http://www.trendmicro.com/NR/rdonlyres/277F8417-34C7-42F3-9A15-713915381F1E/18465/WP01TMMS0020060104US.pdf, [2006, April, 23]

Trost, J. (1997) Kvalitativa intervjuer, Studentlitteratur, Lund.

Wallén, G. (1996) Vetenskapsteori och forskningsmetodik, Studentlitteratur: Lund.

Wayne J., Vlad K. B., Serban G., Thomas H. (2004). A Unified Framework for Mobile Device Security. The National Institute of Standards and Technology, Gaithersburg, USA.

Websense (2005). Protecting Against Complex Internet Threats. Websense, Inc. San Diego, USA. Tillgänglig på http://www.websense.com/docs/WhitePapers/ProtectingAgainstComplexInternetThreats0405.pdf, [2006, April, 12]

Zachary Wilson, (2001) Hacking: The Basics. Tillgänglig på
http://www.sans.org/rr/whitepapers/hackers/955.php, [2006, Maj, 26]