Kandidatuppsats

Sektionen för informationsvetenskap, data- och elektroteknik

Kandidat rapport, IDE 1258, Maj 2012
IT-Forensik och informationssäkerhet

Samhällskonsekvenser

Av bristande IT-säkerhet

Erko Mujanovic, Jan-Ola Stenberg, Frank Stehn

Samhällskonsekvenser

Av bristande IT-säkerhet

Kandidatuppsats

2012 Maj

Författare: Erko Mujanovic, Jan-Ola Stenberg, Frank Stehn

Handledare: Urban Bilstup

Examinator: Mattias Wecksten

Sektionen för informationsvetenskap, data- och elektroteknik
Högskolan i Halmstad
Box 823, 301 18 HALMSTAD

Kandidatuppsats
Rapport, IDE 1258
Sektionen för informationsvetenskap, data- och elektroteknik
Högskolan i Halmstad

Förord

Ett intressant och högaktuellt område att skriva om tyckte vi, innan vi påbörjade vår uppsats, var IT-säkerhet. För att få en spännande och något originell inriktning på vårt arbete valde vi att jobba utifrån teorin att mindre företags brister i IT-säkerheten skulle kunna få konsekvenser för samhället. Vi tänkte från en början inrikta arbetet mer på säkerhetstester och endast inkludera den samhällsvetenskapliga delen som ett mindre diskussionsunderlag. Istället hamnade vi, i takt med att vi utförde intervjuer och undersökningar, nästan helt på spåret att IT-säkerheten hos alla eller många företag kan ha påverkan på samhället. Vi tycker att detta blev en spännande diskussion och vi hoppas att i alla fall någon kommer att få sig en liten tankeställare efter att ha läst vårt arbete.
Vi vill tacka Anders Hansson, Peter Widal och Rickard Hallin för intressant information och diskussion om IT-incidenter, IT-säkerhet och samhällskonsekvenser. Ett stort tack även till vår handledare Urban Bilstrup för vägledning och råd under arbetets gång. Slutligen vill vi tacka Halmstad Högskola för en spännande utbildning och vår examinator och lärare Mattias Wecksten som följt och inspirerat oss under hela vår utbildningstid.

Abstrakt

Antalet företag, organisationer och instanser vars IT-system utsätts för attacker ökar. Något som märks trots att det försöker mörkläggs inom många organisationer. Myndigheter som Polis och Myndigheten för samhällsskydd och beredskap samt IT-personal inom de flesta företag är alla överens om att detta är ett växande problem som måste ses över. Konsekvenser av läckage av känsliga uppgifter kan vara förödande för ett företag, myndighet eller ett helt samhälle. En hel nations demokrati kan hotas av bristande IT-säkerhet och misstro till staten. Görs det tillräckligt för att upprätthålla en säker hantering av känsliga uppgifter och säker kommunikation från alla parter i dagens IT-samhälle? Tar alla sitt ansvar för att bibehålla demokratin vi lever i? Avsätter företagsledningarna på våra svenska företag de resurser som krävs för att IT-säkerheten ska kunna hålla jämn takt med den snabba utveckling i branschen? Tar våra mindre företag sitt ansvar genom att arbeta med IT och informationssäkerhet, trots oförmågan att se sig själva som mål för en attack, eller tillhandahåller de bakdörrar som kan användas av kriminella för att komma åt större företag?

Abstract

The number of companies, organizations and agencies whose IT systems are under attack increases. This is evident even though many organizations tries to hide it. Authorities like the Police, MSP and IT staff in most companies all agree that this is a growing problem that must be reviewed. The consequences of leakage of sensitive data can be devastating to a company, government agency or an entire community. An entire nation's democracy can be threatened by lack of IT security and mistrust of the state government. Is there enough to sustain the safe handling of sensitive data and secure communication of all parties in today's IT community? Does everybody take responsibility to maintain the democracy we live in? Do the managements of our Swedish companies allocate the resources needed for IT security to be able to keep pace with the rapid developments in the industry? Do our smaller businesses take responsibilities by working with IT and information security, despite the inability to see themselves as the target of an attack, or do they provide a backdoor that can be used by criminals to gain access to larger companies?

Innehåll

Figurförteckning

1 Inledning

IT-säkerhet är ett viktigt ämne i dagens IT-samhälle. Tekniken integreras allt mer i människor liv och företag blir allt mer beroende av tekniken för att producera och leverera tjänster och varor. I takt med att IT-tekniken breder ut sig blir vårt samhälle och deras invånare allt mer sårbara för illasinnade enskilda människor, organiserade cyberbrottslingar samt för skadliga programvaror som cirkulerar på Internet. Dessa orsakar, i sin framfart, större eller mindre problem och skada av både ekonomisk samt av samhällskritisk art. IT-säkerhet är ett område vars behov, tror vi, kommer att växa sig allt större i framtiden eftersom tekniken hela tiden går framåt och eftersom vissa människor alltid kommer att försöka stjäla, terrorisera och förstöra. Det blir även allt vanligare att nationer rustar upp sina försvar för att klara av och bemöta attacker som sker i den digitala världen. Eftersom mycket av det moderna samhällets infrastruktur stödjer sig på tekniken utvecklar terrornätverk och krigförande länder strategier i syfte att föra krig med datorer som vapen.[1] Förutom att IT- säkerhet, som tidigare nämnts, är ett viktigt ämne tycker vi, förutom att det också är högst aktuellt, att det är ett väldigt intressant ämne. Det är ett ämne som kräver mycket fokus, kontinuerlig inlärning och ständiga uppdateringar om vad som händer i datorvärlden. Vi har valt att undersöka och diskutera kring mindre svenska företags IT-säkerhet och brister samt vilka konsekvenser detta kan få ur ett samhällsperspektiv. För att uppnå god säkerhet i en IT-infrastruktur finns det många delar man måste jobba med. Vi kommer börja med att ge en kort beskrivning av vad IT-säkerhet innebär, vilka olika delar man bör beakta när man arbetar med den samt ge en kort beskrivning av aktiva säkerhetsanalyser. Vi kommer också belysa vanliga säkerhetsbrister hos företag. Både tekniska och organisatoriska.

I Sverige finns en statlig myndighet som kallas Myndigheten för samhällsskydd och beredskap som har till uppgift att se till att samhällets förmåga att hantera kriser och olyckor ligger på en god nivå samt att stödja samhället vid allvarliga kriser[2]. En gren av förebyggande åtgärder som Myndigheten för samhällsskydd och beredskap ägnar sig åt är informationssäkerhet inom vilken man ger råd och stöd åt myndigheter, kommuner, landsting, företag och övriga organisationer. Förutom siten www.msb.se driver MSB fem stycken andra siter med information om samhällsskydd. En utav dessa fem är www.informationssäkerhet.se, vilken handlar om just IT- och informationssäkerhet. Det faktum att MSB lägger så stor vikt vid just informationssäkerhet tycker vi verifierar vårt tidigare påstående att IT- eller informationssäkerhet är ett viktigt område i dagens samhälle. På www.informa tionssäkerhet.se presenterar MSB ett ramverk för informationssäkerhetsarbete i en verksamhet. Detta ramverk innehåller som

1 Aftonbladet. *En attack kan lamslå landet*, 2011
http://www.aftonbladet.se/nyheter/article12535492.ab

2 MSB. *Myndigheten för samhällsskydd och beredskap*, 2012
http://www.msb.se

andra punkt att analysera verksamhetens IT-system och dess brister[3].

1.1 Bakgrund

Många svenska företag har mindre bra eller ingen kunskap alls om IT- och informationssäkerhet och inte heller någon utarbetad IT-säkerhetspolicy[4]. Man förlitar sig ofta på att antingen den egna IT-avdelningen eller det företag som installerar systemen har tillräckligt bra kunskap inom IT-säkerhet för att verksamhetens system ska vara väl skyddat. Detta anser vi i, många fall, vara helt felaktigt då speciellt mindre och mellanstora IT-företag och konsulter prioriterar användbarhet och tillgänglighet istället för säkerhet. IT-företagens handlande är ofta är helt befogat eftersom priset på installation och drift om man inkluderade välutformad IT-säkerhet i arbetet skulle bli mycket högre vilket företagen som beställer jobben inte har något intresse av att betala för. De förlitar sig på att den grundläggande kunskap systemtekniker och andra tekniker har om IT-säkerhet är tillräcklig. Enligt en undersökning av Saab Combitech utför en tredjedel av företagen aldrig penetrationstester för att säkerställa säkerheten[5]. Även bland företag med ett utbrett säkerhetstänk och som faktiskt har genomarbetade IT-säkerhetspolicys händer att man åsidosätter säkerheten för att erhålla högre tillgänglighet och smidigare arbetsrutiner. Eftersom Sveriges företag är en stor del av det svenska samhället kan det faktum att företagen är dåliga på att skydda sig få negativa konsekvenser för samhället. Det finns en tydlig problematik i att tekniken i samhället ökar utan att fler företag prioriterar IT-säkerhet.

1.2 Syfte

Vi vill med vårt arbete påvisa att IT-säkerhet är bristande samt nedprioriterad hos många svenska företag. Samtidigt vill vi visa upp vilken typ av arbete som kan förbättra IT-säkerheten och vad man bör tänka på i arbetet med denna. Vidare vill vi föra en diskussion om vilka konsekvenser företags bristfälliga IT-säkerhet i förlängningen kan få för samhället samt varför det är viktigt att öka medvetenheten om IT-säkerhet.

1.3 Frågeställningar

1. Finns det några brister i svenska företags IT-miljöer?
2. Hur stor är medvetenheten om IT-säkerhet bland Sveriges företagare?
3. Arbetas det med IT-säkerhet på svenska företag?

---

[3] MSB. *Informationssäkerhet.se - Stöd för verksamheters informationssäkerhetsarbete*, 2010 http://www.informationssäkerhet.se

[4] IDG. *Dåligt med IT-säkerheten bland svenska företag*, 2010 http://www.idg.se/2.1085/1.300997/daligt-med-it-sakerheten-bland-svenska-foretag

[5] IDG. *Så brister svenska företag i IT-säkerhet*, 2011 http://www.idg.se/2.1085/1.422846/sa-brister-svenska-foretag-i-it-sakerhet

4. Vilka konsekvenser kan ett företags bristfälliga IT-skydd i förlängningen få för samhället?

5. Hur påverkas Sveriges medborgare av att samhällskritisk IT-infrastruktur läggs ut på större IT-konsulter?

1.4 Avgränsningar

I diskussionen kring svenska företags IT-säkerhet och deras eventuella påverkan på det svenska samhället kommer vi att göra intervjuer med MSB och ett fåtal mindre företag i Halland. Informationen vi får från dessa kommer att kompletteras med undersökningar och tidningsartiklar inom området och får i vårt arbete gälla som en generell bild av hur säkerheten ser ut hos svenska företag.

1.5 Metod

1.5.1 Stickprov och intervjuer

Vi kommer genom intervjuer att ta stickprov av IT-säkerheten på ett mindre antal lokala företag för att få veta hur svenska företag tänker om IT-säkerheten, på vilken nivå företagen har arbetat med IT-säkerhet samt utifrån dessa uppgifter bilda oss en uppfattning om hur god IT-säkerheten kan tänkas vara hos dessa företag. Utifrån dessa stickprov formulerar vi en teori om hur IT-säkerheten ser ut på svenska företag i stort. Vi kommer vidare att beskriva ett par större IT-incidenter som skett i Sverige samt dess påverkan på det svenska samhället. Fortsättningsvis kommer vi att diskutera hur bristande IT-säkerhet både hos små och medelstora företag samt hos större IT-leverantörer i framtiden kan få allvarliga konsekvenser för samhället i stort.

2 Teori IT-säkerhet och sårbarhetsanalys

2.1 Inledning

Vi vill ge en beskrivning om vilka metoder man som organisation eller företag kan använda sig utav för att säkra upp sina IT-system. För att hålla informationen inom rimliga gränser pekar vi endast på de viktigaste delarna i arbetet med IT-säkerhet samt ger en kort introduktion till dessa.

2.2 Förklaring penetrationstest och sårbarhetsanalyser

Enligt *The Basics of Hacking and Penetration Testing* kan man definiera ett penetrationstest som ett lagligt försök att hacka datorsystem i syfte att göra systemet säkrare[6]. Man utnyttjar befintliga hackerverktyg och skapar sig egna för att på bästa sätt efterlikna en verklig hackerattack i testandet av systemet. Testet ska leda till att man upptäcker eventuella sårbarheter i systemet. Dessa kommer man i ett senare skede även avlägga rapport om samt ge förslag till åtgärd. Boken beskriver också skillnaden mellan ett penetrationstest och en sårbarhetsanalys, vilka annars ofta används synonymt. En sårbarhetsanalys innebär att man analyserar ett system för att hitta potentiella säkerhetshål medan ett penetrationstest tar arbetet ett steg längre genom att utnyttja säkerhetshålet och på så sätt bevisa att säkerhetshålet verkligen existerar.

2.3 Penetrationstestets uppbyggnad

Det finns olika typer av penetrationstest och sårbarhetsanalyser samt lite varierande sätt att utföra dessa. För att få så träffsäkra test som möjligt bör man anlita företag utanför den egna organisationen som testutförare. Testarna har då från starten ingen kunskap om strukturen på systemet som ska testas. Fördelen med detta är att testet får ett verklighetsnära resultat samt att man undviker att testarna påbörjar arbetet med en alltför fyrkantig bild av ett system de redan känner till. Det första en utomstående testare gör när han fått ett uppdrag är att samla in så mycket information om systemet och om företaget, på vilket testet ska utföras, som möjligt. Denna del av testet kallas rekognoscering och är en viktig förutsättning för resterande delar av testet. Testaren fortsätter med att scanna av företagets IT-miljö för att hitta öppna vägar in, ta reda på vilka system som körs samt försöker hitta alla noder som används av företaget. Vidare försöker testaren skapa sig access till de olika systemen. Detta steg kan vara väldigt tidskrävande varför man i en testgrupp med fördel delar upp arbetet mellan testarna. Testarna kan i detta steg även försöka skapa sig access till webbapplikationer och servrar om dessa ingår i testscoopet. Steget efter kan

6 Engebretson, Patrick. *The Basics of Hacking and Penetration Testing - Ethical Hacking and Penetration Testing Made Easy*, Syngress, 2011

innebära, beroende på vad som är överenskommet innan testet, att testarna försöker installera trojaner och rootkits för att verifiera att det går att bibehålla accessen till systemen. Att installera denna typ av bakdörrar är något som de flesta företag vill utesluta i sina tester. Framför allt för att man är rädd att bakdörrarna ska hittas och användas av personer som inte ingår i testgruppen[7]. Slutligen sammanställs informationen från penetrationstestet i en rapport där sårbarheter samt förslag på åtgärder för dessa presenteras. Det finns många olika metoder för att utföra denna typ av tester och fördelaktigt kan vara att använda sig av branschspecifika manualer som till exempel OSSTMM, *The Open Source Security Testing Manual*. OSSTMM används som en gemensam metod för många säkerhetstestare runt om i världen. Med hjälp av manualen får säkerhetstestarna en beprövad metod för analys och ett verktyg för att kunna mäta säkerheten i sina test[8].

2.4 Utbildning

Det viktigaste arbetet med IT-säkerheten är att göra användare av IT-systemen medvetna om vilka risker som finns och hur man bör agera för att undvika dessa. Till den stora skaran användare bör man även inkludera ledning och IT-personal för att erhålla en generell ökning av medvetenhet om IT-säkerhet inom organisationen. I dagsläget spelar det ingen roll hur bra den tekniska säkerheten i ett IT-system är om inte användarna gjorts medvetna om hur de ska använda systemet på ett säkert sätt. Användarna är ofta den största säkerhetsrisken och genom att arbeta med dem vinner man mycket ur ett IT-säkerhetsperspektiv.

2.5 Säkerhetspolicy

Syftet med en IT-säkerhetspolicy är bland annat att klargöra företagets mål med informationssäkerheten, fördela ansvar, förklara regler, definiera en utbildningsplan samt klassificera information och system i olika säkerhetsnivåer. Ofta bygger en säkerhetspolicy på resultatet av en riskanalys med en väldefinierad hotbild. Det är viktigt att man som företag låter sina anställda ta del av IT-säkerhetspolicyn för att minimera riskerna med omedvetna användare.

2.6 Riskanalys

För att veta vilka område inom ett IT-system man behöver säkra upp måste man först utföra en riskanalys. En riskanalys är en beräkning av konsekvenser och sannolikhet för olika incidenter som kan inträffa på ett företag. Beräkningen av konsekvenser kan vara av till exempel ekonomisk eller av samhällsallvarlig typ. Riskanalysen ska ge företaget eller organisationen goda riktlinjer för vilka delar i ett system och vilken information i detta som är av kritisk art. Att identifiera

[7] Whitaker, Andrew. Newman, Daniel. *Penetration Testing and Network Defense*, Cisco Press, 2007

[8] Herzog, Peter. *OSSTMM 3 - The Open Source Security Testing Methodology Manual*, 2010 http://www.isecom.org/mirror/OSSTMM.3.pdf

risker och hot samt konsekvenser av dessa är ett arbete som kräver god kunskap inom såväl IT-säkerhet som om organisationen man analyserar.

2.7 Incidenthantering och kontinuitetsplanering

För att en verksamhet ska kunna möta incidenter på ett tillfredsställande sätt är det viktigt att man planerar för incidenthantering innan incidenten sker. Det är också viktigt att man har en väl fungerande strategi för att upprätthålla verksamheten vid olika typer av för organisationen negativa händelser. Man bör upprätta en plan för incidenthantering som en naturlig del av IT-säkerhetsarbetet. Planen ska innehålla rutiner för allt ifrån hur användare ska rapportera misstänkta incidenter till hur uppföljningen av incidenter ska ske.

3 IT-säkerhet på svenska företag

3.1 Intervju med Richard, säkerhetsansvarig på Motorhalland i Halmstad

Motorhalland är ett medelstort aktiebolag som har funnits sedan 1952. Företaget säljer nya och begagnade bilar, utför service och reparationer på bilar, lastbilar och bussar samt levererar tillbehör och reservdelar till dessa. Motorhalland har ett huvudkontor, ett lager och en verkstad i Halmstad[9].

Under intervjun med Richard berättar han att han anser att Motorhalland har arbetat med IT-säkerheten till viss del, men att det finns en del saker som kan förbättras. Han nämner att alla datorer som används på motorhalland är Windowsmaskiner och att dessa använder antivirusskydd. Till användarkonton finns en lösenordspolicy, vilken är konfigurerad så att varje användare måste ha lösenord bestående av tre stycken stora bokstäver och tre stycken siffror. Lösenorden för användarna behöver inte bytas någon gång utan används tills den dag personen slutar jobba på Motorhalland. Han medger att lösenords-kombinationen inte anses säker, men antyder att det ser ut på detta sätt eftersom användarna hade svårigheter att komma ihåg mer avancerade lösenord som de tidigare blev tilldelade. Skulle lösenorden vara mer komplicerade, med en blandning av specialtecken, stora bokstäver, små bokstäver och siffror så hade det slutat med att användarna skulle lägga små lappar med lösenord under tangentbord, på skärmar eller liknande. Han säger även att Motorhalland använder sig av logganalys så att oönskad aktivitet på användarkonton upptäcks. När en användare tar semester eller långledigt inaktiveras inte användarkontona säger Richard. Han medger också att användarna aldrig utbildats för att öka säkerhetsmedvetenheten eller för att minska riskerna inom IT-miljön.

De servrar som Motorhalland använder är lokaliserade i ett rum på huvudkontoret. Rummet är låst och även larmat på natten. Det finns även brandväggar mellan Internet och det interna nätet. All trafik stannar inom det interna nätet så länge ingen ansluter sig till Internet. Motorhalland har tillgång till några leverantörs-system och i dessa använder man sig av certifikat för att komma åt säger Richard.

Motorhalland är delägare i det företaget som har hand om IT-säkerheten i Motorhallands system. Varje natt utförs säkerhetskopiering på hårddiskmedia samt görs en backup till bandhårddiskar en gång per vecka. Banden placeras i ett brandskåp i samma lokal som servrarna. Richard säger även att systemen som används uppdateras en till två gånger i veckan och detta utförs av personal på huvudkontoret.

---

9 Motorhalland. *Motorhalland*, 2012
http://www.motorhalland.se

Skulle en incident inträffa och påverka verksamheten negativt till följd av bristande IT-säkerhet skulle Richard se detta som mycket allvarligt. Detta skulle medföra att anställda inte skulle kunna jobba som vanligt, vilket i sin tur skulle resultera i att företaget skulle tjäna mindre pengar.

3.2 Intervju med Peter, VD på Widal Industri i Getinge

Intervju med Peter Widal, delägare och VD på Widal Industri i Getinge. Widal Industri AB är ett mindre företag på 19 anställda inom metallindustrin som utför diverse plåtarbeten som svetsning, slipning, skärning, kantpressning, montering samt mycket annat. Metall är inte det enda materialet man på Widal industri arbetar med utan även material så som gummi, plast och kolfiber bearbetas på företaget[10]. Maskinerna som används på Widal industri AB drivs alla av servar som står i specifika utrymmen i fabriken och dessa utrymmen saknar säkerhet medger Peter.

Under intervjun med Peter Widal på Widal Industri AB så framkom det att det inte fanns så mycket tänk kring just IT-säkerhet inom företaget. Man anser att det i dagsläget inte finns tillräckligt stora risker och hot mot IT-miljön för att det ska vara lönsamt att spendera resurser på området. På frågorna om det finns någon it-säkerhetspolicy, utbildning inom IT-säkerhet till användare och om det finns något skydd för det rum som används för datordrift så svarade Peter att inget av detta har dem tänkt på då de anser att varken hot eller risker är speciellt stora. På Widal Industri AB förlitar man sig helt och hållet på sin nätverksleverantör, Media Network, vad gäller allt kring IT. Säkerheten inkluderad. Media Network erbjuder på sin hemsida IT-tjänster som service, installation, serverdrift och även försäljning av hårdvara men nämner inte mycket om IT-säkerhet[11].

Att ha en person anställd som IT-ansvarig i dagsläget anser man vara för dyrt även om man är medveten om IT-teknikens utveckling och tror att man i framtiden kommer behöva anställa någon inom området. På Widal Industri är man väl medvetna om att det i dagsläget finns brister i IT-säkerheten. Till exempel så finns det inte någon långsiktigt strategisk planering kring företagets IT-säkerhet och det ställs inte några säkerhetskrav på samarbetspartners. Widal Industri har heller inte några krav på sig själva. Detta försvarar man återigen med att man inte anser hotet vara tillräckligt stort. Några egentliga företagshemligheter tycks man inte ha och att någon skulle vilja sabotera just deras verksamhet verkar otänkbart. Man försvarar sin brist på IT-säkerhet medvetet och omedvetet med argumentet varför skulle det hända just oss? Backup av information utförs varje dag och detta stoltserar Peter med då han vet

---

10 Widal Industri AB. *Widal Industri AB - vattenskärning, trycktankar, licenssvetsning*, 2012 http://www.widalindustri.se/?pid=28&sub=24

11 Media Network. *Medianetworks.se*, 2012 http://www.medianetwork.se/

att många liknande företag inte ens gör detta.

3.3 Diskussion

Är IT-säkerheten bristfällig hos de svenska företagen och vad beror i så fall detta på? Är det ett globalt problem eller är det bara vi i Sverige som är så okunniga inom området? Detta är en del utav de frågor som många IT-analytiker och säkerhetsexperter lägger stor tyngd vid och belyser dagligen i syfte att öppna upp ögonen för företagsledningar och få dem att förstå vikten utav IT-säkerheten. Brister inom området uppdagas näst intill dagligen och det visas även exempel på de negativa konsekvenser företagen får till följd IT-relaterade incidenter. Även privatpersoner drabbas av IT-incidenter.

Artiklar om IT-attacker mot svenska företag ökar markant i media. Detta trots att företagen oftast försöker att mörklägga incidenterna för att skydda verksamhetens rykte. Företagets varumärke och kundernas tillit till varumärket kan skadas om det uppmärksammas i media att känslig information stulits. Dessa aspekter gör att även företagsledningar inser hur viktigt det är för företaget att informationssäkerheten håller hög standard och inga företagshemligheter läcker ut. Trots detta så är det många som blundar för användning av privata enheter så som mobiltelefoner och USB-minnen på arbetsplatsen och enbart var femte företag har som policy, även ifall inte denna alltid följs, att förbjuda privata enheter på arbetsplatsen enligt en undersökning genomförd av Saab Combitech. Enligt samma undersökning är det bara en fjärdedel av alla företag som har en fullgod rutin för att utföra riskanalyser kontinuerligt, säger Magnus Kårenda, affärsområdeschef på Combitech. En tredjedel av företagen gör aldrig något penetrationstest på sitt IT-system och loggar analyseras bara av knappt vart femte företag och detta sker enbart efter en incident hos 40 procent av företagen enligt Combitechs undersökning[12]. Det är hela 6 av 10 ledningsgrupper inom olika företag som har en väldigt överskattad bild utav sitt IT-säkerhetssystem. I de fall IT-cheferna vill lägga resurser på att säkra upp sitt system får de oftast otillräckligt stöd från ledningen. Detta visar undersökningar analysföretaget Gabriel Consulting Group utfört på anvisning utav McAfee och CA Technologies. Undersökningen som gjordes på uppdrag av McAfee innefattade 147 IT-ledares synpunkter och åsikter på företag främst i USA och Europa[13].

Är okunnighet den faktor som gör att detta sker och fortlöper hos våra svenska företag eller är det återigen den ekonomiska biten som är den bidragande orsaken. Eller kan det bara vara så att människan av naturen är sådan att hon blundar för och förtränger problem tills de faktiskt drabbar henne själv. Vid förlust av till exempel ett företags bärbara dator kan den ekonomiska förlusten

---

12 IDG. *Så brister svenska företag i IT-säkerhet*, 2011
http://www.idg.se/2.1085/1.422846/sa-brister-svenska-foretag-i-it-sakerhet

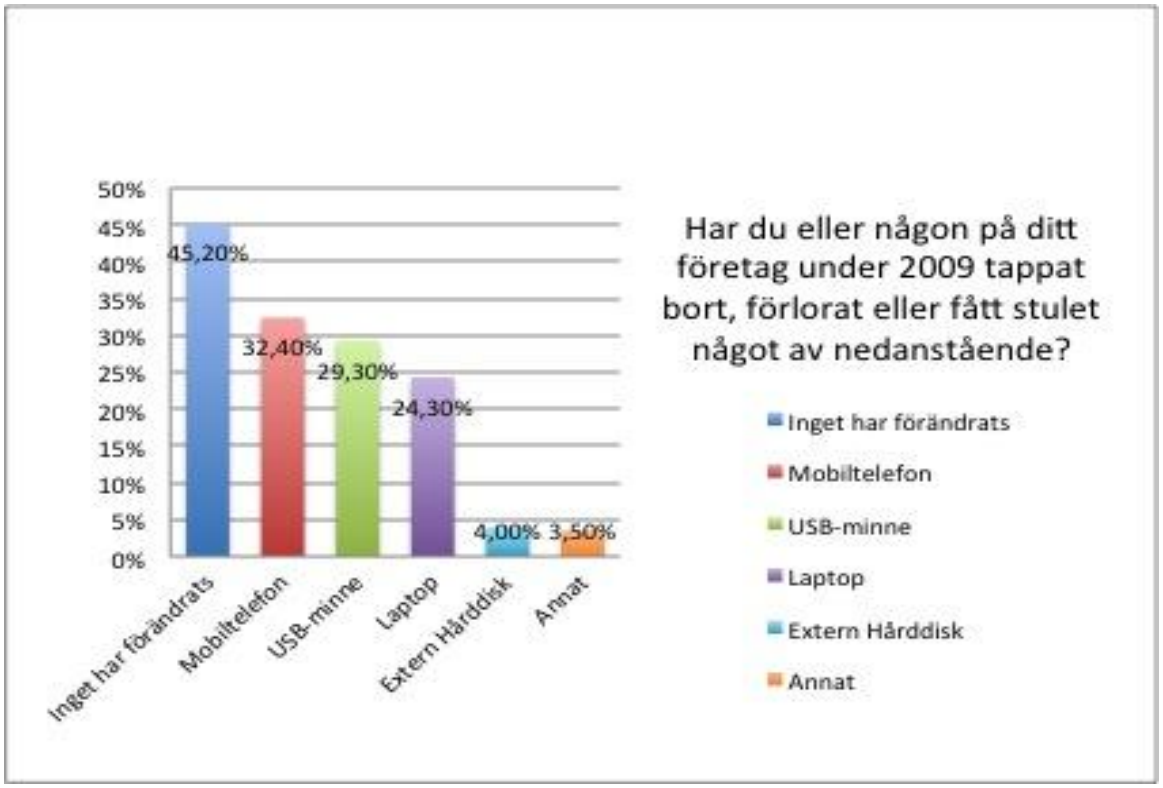
13 IDG. *Ledningen svävar i det blå om IT-säkerhet*, 2011
http://www.idg.se/2.1085/1.409133/ledningen-svavar-i-det-bla-om-it-sakerhet

för företaget långt överstiga den faktiska kostnaden för den bärbara datorn. Detta eftersom datorn även kan innehålla känslig information som är betydligt mer värdefull för företaget än själva hårdvaran.

Enligt Cryptzone Groups svenska IT-säkerhetsundersökning från 2009 har nästan 55 procent av de tillfrågade vid något tillfälle blivit bestulna på eller tappat bort antingen USB-minnen, mobiltelefoner, laptops, externa hårddiskar eller andra enheter med företagsinformation[14].

Figur 1(Datakälla: Cryptzone)

Hur vanliga dataförluster är hos de svenska företagen är svårt att säga eftersom de flesta företag inte går ut med dessa uppgifter offentligt. I Sverige finns ingen anmälningsplikt vid IT-incidenter i motsats till vissa delstater i USA som säger att



informationsläckage hos företag om tredjepart måste rapporteras. Allt för många företag runt om i Sverige saknar en utarbetad IT-säkerhetspolicy alternativt inte följer de skrivelser som företaget tagit fram gällande IT- och informationssäkerhet.

Cryptzones VD Peter Davin säger i en intervju med TechWorld Säkerhet att problematiken ofta ligger i bristande förståelse hos företagsledningen. Det är

14 IDG. *Dåligt med IT-säkerheten bland Svenska företag*, 2010 http://www.idg.se/2.1085/1.300997/daligt-med-it-sakerheten-bland-svenska-foretag

ledningen som måste inse allvaret för att en förändring ska kunna komma till stånd. IT-avdelningen är oftast tillräckligt kunniga för att kunna inse problematiken med bristande säkerhet och har en vilja att förbättra denna. För att detta ska kunna ske krävs medhåll från ledningens sida[15].

[15] IDG. *Dataläckage är en ledningsfråga*, 2010
http://sakerhet.idg.se/2.1070/1.301164/datalackage-ar-en-ledningsfraga

4 Samhällskonsekvenser av bristande IT-säkerhet

4.1 Intervju med Anders Hansson, ställföreträdande chef på avdelningen CERT-se inom MSB

Myndigheten för Samhällsskydd och Beredskap, MSB, finns till för att stödja samhället vid kriser och olyckor[16]. Deras uppgifter inkluderar också att se till att samhället arbetar med förebyggande åtgärder för denna typ av händelser, att samhället är förberedda för händelserna samt att samhället lär sig av händelserna när de väl inträffat. MSB driver ett antal informativa siter varav en är siten informationssäkerhet.se, vilken ska fungera som stöd för verksamheters IT-säkerhetsarbete. Siten presenterar bland annat ett ramverk för IT-säkerhet, vägledning inom IT-säkerhetsfrågor samt rapporter om IT-incidenter[17].

Vi pratade med Anders Hansson vid MSB för att ta reda på hur IT-säkerheten ser ut hos svenska företag samt vilka konsekvenser MSB ser att bristande IT-säkerhet hos företagen får för samhället. På frågan om hur IT-säkerheten ser ut hos svenska företag svarar Anders att han tror att medvetenheten hos Sveriges företagare är högre än hos företag i andra länder. Trots detta varierar kvalitén på IT-säkerheten även i Sverige berättar Anders. Han förklarar att den absolut vanligaste typen av attacker är de av typen *Denial Of Service*, eller *Distributed Denial Of Service*, och att syftet med dessa attacker ofta är av politisk art eller att på något sätt visa sitt missnöje. Denna typ av attacker utförs även för att sabotera för konkurrenter och för att utpressa företag på pengar. Anders säger att mörkertalet för IT-incidenter förmodligen är mycket stort, både på grund utav av att företag ofta håller inne med information om dessa för att inte få dåligt rykte, men också på grund utav att många attacker, till exempel datorintrång, aldrig upptäcks av företagen. När vi frågar Anders hur han tror att dålig IT-säkerhet på mindre företag påverkar samhället i stort svarar han att framför allt den ökade outsourcingen i Sverige gör att IT-säkerheten kan bli sämre hos många företag. Det man normalt sett tittar på när man köper outsourcingtjänster är tillgänglighet och pris vilket gör att IT-säkerhet, i många fall, inte ens finns omnämnt i de avtal man tecknar. Han säger också att det är en kostnadsfråga och att många företag väljer bort IT-säkerhet eftersom den ger just en ökad kostnad. Vidare berättar Anders att han tycker att fler företag borde testa sina system och även att de som gör det idag borde utföra fler tester. Vi frågar Anders vad man kan göra för att öka medvetenheten kring IT-säkerhet hos svenska företagare. Han svarar att bra tillvägagångssätt för detta är att demonstrera olika händelser inom hacking. Vidare berättar han att företagen bör inkludera utbildning i sina IT-säkerhetssatsningar samt att det redan idag finns många företag som utbildar sina anställda inom området. Han berättar också att det börjar bli extra svårt att

16 MSB. *Myndigheten för samhällsskydd och beredskap*, 2012 http://www.msb.se

17 MSB. *Informationssäkerhet.se*, 2012 http://www.informationssakerhet.se

hålla koll på säkerheten i och med intåget av så kallade smartphones. På frågan ifall svenska företag har ett ansvar gentemot samhället svarar Anders att de flesta har någon typ av ansvar eftersom de är en del av samhället. Han tycker dock att myndigheterna har ett större ansvar än företagen eftersom dessa tillhandahåller viktiga samhällsfunktioner. Det finns även företag som tillhandahåller viktiga samhällsfunktioner och gällande dessa tycker Anders man bör utgå ifrån närhetsprincipen. Det vill säga att den närmast ansvariga för funktionen också är den som har det faktiska ansvaret. Vidare berättar Anders att det finns ett antal viktiga stödfunktioner när det gäller IT-säkerhet som till exempel Polisen och MSB. Misstänker man att IT-relaterade brott begås så finns det ett antal funktioner inom samhället som kan hjälpa till att förhindra och förebygga dessa. Det är viktigt att man rapporterar brotten för att kunna avhjälpa dem. Som det ser ut idag, berättar Anders, finns det ett stort mörkertal inom IT-relaterade brott eftersom man ser det som skamligt att ha blivit utsatt för brott och man är samtidigt rädd att det ska ge negativ publicitet. Detta gäller alla funktioner i samhället säger han. Vi avslutar med frågan om vilken myndighets eller vilket företags IT-infrastruktur som är den mest samhällskritiska. Anders berättar att det är en omdiskuterad fråga utan något egentligt bra svar. Han spekulerar kring om det är elbolagen, telebolagen eller reningsverken som har den mest kritiska funktionen i samhället. Mycket är beroende av IT idag och det finns en stor brist i samhället vad gäller ansvarsfördelning, kontinuitetsplanering och säkerhetsarbete berättar han.

4.2 Haveriet hos Tieto

Tieto är enligt egen utsago norra Europas ledande leverantör av IT- och produktutvecklingstjänster och på deras webbsida kan man läsa att behovet av ständigt tillgängliga tjänster, som kan användas oberoende av tid eller plats, ökar kontinuerligt[18]. Vidare kan man läsa att Tieto verkar inom den offentliga sektorn och säljer IT-tjänster till offentliga företag och myndigheter. I november 2011 drabbades Tieto av ett omfattande haveri vilket påverkade ett femtiotal av de kunder som lagt ut sin IT-drift på Tieto[19]. Bland dessa fanns ett flertal företag från den offentliga sektorn och bland dem flera med viktiga samhällsfunktioner. Apoteket, Svensk Bilprovning, SBAB och Socialstyrelsen är exempel på några av de företag som drabbades av haveriet[20]. Enligt MSB vägrade Tieto lämna ut uppgifter om vilka myndigheter som drabbades av haveriet med hänvisning till affärssekretessregler vilket har inneburit att det inte finns några exakta uppgifter på vilka myndigheter som faktiskt blev drabbade[21]. Orsaken till det fem

18 Tieto. *Tieto på 2 minuter*, 2012
http://www.tieto.se/om-oss/tieto-pa-2-minuter

19 MSB. *Reflektioner kring samhällets skydd och beredskap vid allvarliga IT-incidenter*, 2012
https://www.msb.se/RibData/Filer/pdf/26170.pdf

20 Magnusson, Anders. *Lärdomarna efter Tieto-kraschen*, 2012
http://www.telekomidag.se/nyheter/artikel.php?id=37469

21 Zirn, Tomas. *Tieto mörkade även för MSB*, 2012
http://computersweden.idg.se/2.2683/1.434213/tieto-morkade-aven-for-msb

veckor långa haveriet var enligt Tieto ett hårdvarufel. Något som heller inte kan bekräftas eftersom Tieto inte släppt in utomstående i utredningen.

4.3 Intrånget hos Logica

På Logicas webbsida kan man läsa att företaget är ett ledande internationellt IT-tjänsteföretag med 41 000 medarbetare, varav 5 200 i Sverige[22]. De erbjuder bland annat verksamhetsinriktade konsulttjänster, systemintegration och outsourcing till många av Europas största företag och organisationer. Även bland Logicas kunder hittar man myndigheter och företag med viktiga samhällstjänster. Skatteverket, Polisen, Försäkringskassan och kronofogdemyndigheten är några exempel på dessa. Skatteverkets folkbokföringsregister innehåller känsliga uppgifter om de flesta av Sveriges medborgare, sekretessklassad information om brottsoffer samt information om personer som utsatts för hot i samband med vittnesmål[23]. Det är av uppenbarliga skäl väldigt viktigt att denna information hålls hemlig. Inte bara för de utsatta personerna och deras närstående men även ur ett samhällsperspektiv för att kunna bibehålla en demokratisk ordning i landet. Demokrati och rättsäkerhet kräver en trygg miljö för medborgare att vittna i.

Logica drabbades våren 2012 av ett datorintrång vid vilket man tror att hackare kom över tusentals personuppgifter och bland dessa över tusen personnummer för personer som lever med skyddad identitet[24]. Exakt vilka uppgifter som stals vid intrånget är oklart men ärendet utreds i skrivande stund av Länskriminalpolisen. Visar det sig att detaljerade personuppgifter för människor som lever under skyddad identitet stulits är detta naturligtvis en väldigt allvarlig händelse. Vissa av dessa personers liv hänger på att deras identitet förblir hemlig och samtidigt kan händelser av denna typ förstöra människors förtroende för rättsväsendet vilket i förlängningen kan få förödande konsekvenser för samhället.

4.4 Diskussion IT-säkerhet och samhällskonsekvenser

4.4.1 Större IT-leverantörer

Med anledning av tidigare nämnt haveri hos IT-leverantören Tieto sammanställdes en rapport av MSB i syfte att belysa samhällskonsekvenser av allvarliga IT-incidenter[25]. I rapporten framhäver MSB vikten av ett nationellt

---

22 Logica. *Mer om Logica*, 2012
http://www.logica.se/we-are-logica/about-logica/

23 Holmén, Christian. *Hackerattack mot skatteverket*, 2012
http://www.expressen.se/nyheter/hackerattack-mot-skatteverket/

24 Videla, Emanuel. *Hackare kom över Skatteverkets hemliga uppgifter vid intrång*, 2012
http://computersweden.idg.se/2.2683/1.440895/hackare-kom-over-skatteverkets-hemliga-uppgifter-vid-intrang

25 MSB. *Reflektioner kring samhällets skydd och beredskap vid allvarliga IT-incidenter*, 2012
https://www.msb.se/RibData/Filer/pdf/26170.pdf

samarbete mellan både offentliga och privata aktörer inom området informationssäkerhet med anledningen av den ökande koncentrationen av IT-drift och andra IT-relaterade tjänster. För att minska konsekvenserna av IT-incidenterna, berättar MSB i rapporten, bör man framför allt koncentrera sig på riskanalys och kontinuitets-planering. MSB belyser också riskerna med att flera myndigheter med viktiga samhällsfunktioner använder sig av samma IT-leverantör. En incident hos leverantören kan få konsekvensen att alla dessa viktiga samhällsfunktioner försvinner samtidigt, vilket i sin tur kan få allvarliga konsekvenser för ett samhälle som stödjer sig mot informationsteknologi i den omfattning det svenska samhället gör. Det har skrivits mycket på senare tid om att företag mer och mer börjar använda molntjänster och outsourcing i sina verksamheter.

Enligt en undersökning av CIO Sweden och Combitech outsourcar två tredjedelar av svenska företag IT-tjänster. Undersökningen säger även att nästan hälften av dessa som outsourcar använder sig även av molntjänster för system och affärsprocesser. Endast en fjärdedel av företagen har tillräckligt med rutiner för att hantera riskanalyser och dessutom utför tre av tio företag aldrig penetrationstester för att upprätthålla säkerheten hos IT-infrastrukturen[26].

Med outsourcing menas att ett företag anlitar ett annat företag som tar hand om olika tjänster eller produkter för att underlätta för företagets verksamhet. Det finns både för och nackdelar med att lämna över arbetet till ett annat företag, vilka man får väga emot varandra för att få reda på om outsourcingen kommer att skapa mer lönsamhet i verksamheten. Den största anledningen till att företag använder outsourcing är att man inte hinner med att sköta driften själv, inte har tillräckligt med kunskaper för att uppehålla hög kvalité eller för att spara in pengar. Det är därför en fördel att kunna lämna över det till företag som är specialister, har mer kompetens inom området samt utför arbetet till ett reducerat pris. Detta medför att man spar in pengar på att inte behöva anställa personal, betala skatt och på andra sätt ta av företagets resurser. Men att låta ett annat företag utföra ett arbete kan vara riskabelt då delning av känslig data kan förekomma och därmed kan säkerheten stå på spel.

Ett datormoln består av en grupp resurser, såsom lagring, processorkraft och andra funktioner vilka oftast är uppkopplade till internet. Det faktum att delar eller hela nätverket kan flyttas ut på internet gör att andra företag kan sköta driften av dessa och erbjuda tjänster såsom datalagring. Dropbox och Google Drive är tjänster som använder sig av datormolntekniken och har blivit stora och populära på senaste tiden.

Det finns en hel del oro kring IT-säkerheten i molntjänster. Trots detta blir dessa tjänster mer och mer populära. Enligt en undersökning som gjordes av Symantec

---

26 Combitech. *Brister i säkerhetsberedskapen hos Svenska företag*, 2011 http://www.combitech.se/sv/Om-Combitech/Nyheter-press-och-media/Nyheter-och-pressmeddelanden/2011---12/Brister-i-sakerhetsberedskapen-hos-svenska-foretag/

visade det sig att cirka hälften av alla företag redan börjat använda sig av molntjänster av något slag.[27] Vissa företag hade enligt undersökningen redan börjat flytta över ett antal applikationer till externa molnservrar och även till privata moln. Det finns även företag som använder privata och offentliga molntjänster som är sammankopplade. Företagen ser molntjänster som en chans till ökad flexibilitet och effektivitet, lägre driftkostnader, förbättrad katastrofåterställning och dessutom en ökad säkerhet.

Det finns ett flertal olika företag som inte tar IT-säkerheten på allvar förrän det väl inträffar en incident. Förra året, juni 2011, granskades IT-säkerheten på svenska universitetssjukhus, vilka visade sig att säkerheten var bristfälliga.[28] På dessa sjukhus var säkerheten så dålig att patientsäkerheten var hotad enligt Socialstyrelsen. Av de sex sjukhus som granskades var det inte något som klarade sig undan utan kritik mot deras säkerhet. Deras säkerhetsproblem berodde på bristande ansvar från sjukhusens ledningar. Det som kritiserades var bland annat att journalsystemen vid driftstopp räknar fram felaktiga läkemedelsdoser.

Även stora Internetleverantörer råkar ibland ut för incidenter och vissa av dessa påverkar samhället i stor utsträckning. Internetleverantören Comhem, hade ett stort säkerhetshål januari 2012, vilket orsakade att 140 000 bredbandskunder drabbades.[29] Minst en modemmodell som Comhem gav till sina kunder hade funktionen WPS-PIN påslaget som standard och lösenordet var samma på alla modem, 12345670. Detta gjorde det möjligt för inkräktare såsom hackers att enkelt ansluta sig till modemet genom att ange det välkända lösenordet

Brist på säkerhet och upptäckter av säkerhetshål har ett flertal gånger drabbat både små och stora IT-leverantörer. Stora IT-leverantörer bör ha mer resurser att satsa på säkerhetsarbete och även ha en bättre säkerhetsplanering än små företag, men i många fall är detta tyvärr inte sant. Alla företag kan råka ut för IT-incidenter, men för att bemöta dessa på bästa sätt samt för att i möjligaste mån undvika dem bör man utforma säkerhetspolicys, utföra riskanalyser samt penetrationstesta systemen med jämna intervaller.

De flesta företag ser inte riskerna förrän en incident väl har inträffat vilket kan påverka samhället negativt. Skulle det visa sig att en bank har ett dåligt säkerhetstänk så kan samhället drabbas av panik vilket i sin tur kan medföra att banken går i konkurs. Att det skulle bryta ut samhällspanik som en följd av att stora IT-leverantörer råkar ut för incident är inte helt otänkbart eftersom

[27] IDG. *Fler väljer molntjänster trots frågor om säkerhet*, 2011 http://cloud.idg.se/2.16150/1.411389/fler-valjer-molntjanster-trots-fragor-om-sakerhet

[28] IT i vården. *Svenska universitetssjukhus har bristande IT-säkerhet*, 2011 http://itivarden.idg.se/2.2898/1.392484/svenska-universitetssjukhus-har-bristande-it-sakerhet

[29] IDG. *Comhem: Stort säkerhetshål drabbar 140 000 bredbandkunder*, 2012 http://www.idg.se/2.1085/1.426980/comhem-stort-sakerhetshal-drabbar-140-000-bredbandskunder

myndigheter med viktiga samhällstjänster ofta huserar på större IT-leverantörers system.

För att undvika att alla dessa viktiga samhällsfunktioner påverkas samtidigt om en stor IT-leverantör får problem borde funktionerna delas upp på olika IT-leverantörer alternativt borde funktionerna finnas redundanta på flera leverantörer. Skulle då något tekniskt problem inträffa så påverkas inte alla banker, el- och vattenbolag samtidigt utan man kan då minimera påverkan på samhället och undvika kriser.

4.4.2 Små och medelstora företag

Är en bristfällig IT-säkerhet hos småföretag av så stor betydelse att konsekvenserna lämnar avtryck på samhället i en större omfattning eller blir denna påverkan minimal? Att stora globala företag som till exempel Sony, Microsoft och Volvo vars årliga omsättning ligger på flera miljarder svenska kronor[30] har en stor samhällspåverkan finns det ingen tvekan om. Att dessa företag måste ha en hög IT-säkerhet och skydda deras värdefulla information och IT-system är en självklarhet. Frågan som istället bör ställas är hur alla de mindre företagen som är underleverantörer till dessa jättar arbetar för att upprätthålla IT- och informationssäkerheten inom sina system. Ställs det några krav på standarden för små företags IT- och informationssäkerhet från de stora globala företagen som de är underleverantörer till?

Att upprätta en bra IT-säkerhet brukar oftast påverkas av en specifik faktor och det är den ekonomiska faktorn. Mindre företag brukar se säkerhetsarbetet endast som kostnader vilket därför ofta nedprioriteras. Oftast har inga uträkningar gjorts över vad kostnaderna blir vid ett eventuellt behov av till exempel backuper på arbeten om där inte finns några eller hur värdefulla affärshemligheter och kundregister kan vara. Datamängden och behovet av ett välfungerande IT-system hos de svenska småföretagen ökar markant, i samband med detta stiger även värderingen av ett säkert IT och informationssystem[31]. Trots detta så är det många företagsledningar som inte tar frågan på allvar och inte avsätter tillräckligt med ekonomiska resurser för IT-säkerheten.

Många företagsledningar resonerar på så sätt att de inte anser den information de har vara så pass känslig att någon annan skulle vilja komma över den. Tankarna på att arbeta i förebyggande syfte finns inte och man anser inte risken vara tillräckligt stor för de skulle utsättas för brott som till exempel datorintrång. Det många företagsledningar inte tänker på är att en person som utför sabotage mot företaget inte behöver ha just det företaget som måltavla utan kanske någon

[30] Avanza bank. *Volvo står starkt*, 2006
https://www.avanza.se/aza/press/press_article.jsp?article=5360

[31] Mynewsdesk. *Småföretag brister i datasäkerhet*, 2010
http://www.mynewsdesk.com/se/pressroom/it-hantverkarna/pressrelease/view/smaafoeretag-brister-i-datasaekerhet-haelften-saekerhetskopierar-aldrig-utanfoer-hemmet-466188

samarbetspartner till detta företag. Precis som vi tidigare konstaterat så har de stora företagen både kunskapen och de ekonomiska resurserna för att hålla en hög standard på deras IT- och informationssystem. Då de ofta finns utspridda över riket och ibland världen över så har de även insett vikten av ett väl fungerande IT-system för att kommunikationen inom företaget och mellan de olika avdelningarna ska fungera. Därför värderas och prioriteras detta väldigt högt. För att kunna ta sig förbi de stora företagens system så krävs både kunskap och tillgångar då företagen lagt ner mycket ekonomiska resurser och har kunskap om att förhindra intrång.

Det är betydligt enklare för en person eller organisation vars mål är att sabotera att rikta in sig på just mindre företag som är underleverantörer till de större företagen. Detta med anledning av att de företagen inte prioriterat säkerheten inom systemet lika högt då ekonomin och kunskaper inom företagsledningen saknas[32]. Som ett mindre företag förväntar man sig inte vara målet för en sådan attack och har därför inte lagt ner samma resurser i förebyggande syfte. Därför blir bristande IT-säkerhet hos småföretag en faktor som påverkar samhället. Påverkan blir kanske inte lika direkt som om det skulle röra sig om attacker mot till exempel Volvo eller något stort företag som tillverkar mediciner. Dock så påverkas de indirekt då attacken sker mot ett mindre företag som levererar tjänster och produkter åt de större företagen. Detta i sin tur slår mot resten av samhället och dess invånare. Slagkraften hos en sådan attack kan resultera i att apoteken och sjukhusen inte har läkemedlen som behövs eller att Volvo inte får ut sina bilar i tid.

Den illasinnade individen vars mål är att terrorisera samhället eller sabotera för ett företag får nästan samma effekt av sina handlingar gentemot samhället och företaget. För att lyckas med attacker mot mindre företag krävs inte fullt lika mycket resurser eller kunskaper. Ser man som mindre företag problemet från denna synvinkel så kanske man ser sig själv som en betydligt större måltavla och inser att möjligheten för att utsättas för en sådan attack faktiskt finns där.

Detta kan framstå som små bekymmer i dagens samhälle och argumentet att det enda som egentligen sker är att leveransen av Volvos bilar försenas kan tyckas giltigt, men tyvärr kan effekterna bli värre än så och i vissa fall näst intill förödande för samhället. Problematiskt är också att det inte krävs stora resurser och djupa kunskaper för att lyckas med en sådan attack vilket gör att ett stort antal personer är kapabla till att utföra attacken. Detta kan innebära att till och med en tonåring med bara ett visst datorintresse kan sitta i skolan på sin rast och utföra detta för skojs skull vilket kan medföra stora konsekvenser för de drabbade. Ges en chans åt fel person till insyn och åtkomst till ett företaget så finns det egentligen ingen gräns på hur förödande denna attack kan vara för samhället och människorna. Av många ses mindre företagen, och underleverantörer, med sämre säkerhet, som en bakdörr in i större system.

[32] IDG. *Många småföretag känner sig otrygga med säkerheten*, 2007 http://www.idg.se/2.1085/1.108964

Vad kan man egentligen att göra för att förhindra detta? Har de stora globala företagen rätt att ställa hur mycket krav som helst på de mindre underleverantörerna trots deras mindre ekonomiska resurser.

I takt med att cybervärlden utvecklas så ökar även brottsligheten inom den och skyddar vi då inte oss på rätt sätt kan det medföra stora risker för samhället. Småföretagen måste inse att deras egna handlingar och säkerhet kan starta en kedjereaktion som påverkar andra företag i slutändan hela det svenska samhället. I en värld med ett samhälle som är så globaliserat som det vi lever i måste vi inse att våra handlingar i många fall kan innebära konsekvenser för fler parter än oss själva.

Oavsett hos vem ansvaret ligger i dagsläget så kan vi inget annat än konstatera att framtiden kommer att tvinga oss säkra våra IT-system och vi kommer att behöva rekrytera kunnig personal inom området. Viktigt för företagsledningen är att inse vikten av ett uppdaterat och välfungerande system med en skräddarsydd incidentplanering och en glasklar IT-policy[33]. För att kunna tillgodose säkerhets-behovet måste IT-avdelningen förses med de resurser de behöver. Då teknikerna moderniseras och känsligare uppgifter behandlas på datorer, servrar och olika nätverk så medför detta även ansvar hos företagen. Man måste först och främst förstå hur känslig den informationen man lagrar kan vara samt förstå vilka konsekvenser det kan få ifall den hamnar i fel händer. Som en del av ett samhälle, vilket alla företag, individer, organisationer och föreningar är, så måste man förstå och ta sitt ansvar gentemot sin omgivning och resten av samhället.

5 Slutsats

Frågan om huruvida det är möjligt att sätta ihop ett helt säkert IT-system hos något företag är svårt att svara på men oavsett svaret på den frågan så kan man göra mycket för att förbättra säkerheten i ett system. Med den utveckling vi idag har inom IT-världen så är det viktigt att företagen ur en säkerhetsaspekt håller jämna steg med utvecklingen hos cyberkriminella. Företagsledningar måste inse att där finns risker för att bli utsatta för en attack och avse mer ekonomiska resurser till IT-avdelningen och IT-säkerhetens utveckling inom företaget. Svenska företag, oftast mindre och medelstora behöver bli mer säkerhetsmedvetna och de behöver skapa riktlinjer för IT-säkerheten i form av en säkerhetspolicy. Denna säkerhetspolicy måste finnas och följas i varje företag för att den ska få en positiv effekt för generell säkerheten i samhället. De olika IT-systemen inom de flesta företag och myndigheter får en allt större och viktigare roll och krävs för en fungerande organisation. Då man i dagsläget använder sig av datorer på varje företag och allt mer känsliga uppgifter hanteras inom systemen måste även mer vikt läggas på säkerheten inom dessa system.

[33] IDG. *Många småföretag känner sig otrygga med säkerheten*, 2007 http://www.idg.se/2.1085/1.108964

Samhällskonsekvenser av bristande IT-säkerhet

Brister inom säkerheten av IT-systemen är inte enbart något som förekommer hos de mindre företagen utan finns hos större företag också. Det är ingen lätt uppgift att hålla jämna steg med den ständiga utvecklingen inom IT-världen. När fler företag blir beroende av sina IT-system och använder sig utav dem så skapas där även brister och kryphål som den illasinnade individen kan utnyttja. Företagsledningar och användarna av IT-systemen måste se potentiella konsekvenserna av bristfällig IT-säkerhet för att kunna förstå vikten av en välfungerande säkerhetsstrategi. Vi måste därför ha rätt utbildad personal inom detta område som ofta nedprioriteras men som är så viktigt för företagen och samhället.

Som vi tidigare nämnt har ett flertal IT-incidenter hos större IT-leverantörer uppmärksammats i media. Dessa incidenter har fått konsekvenser för samhället i form utav att flera viktiga samhällsfunktioner varit ur bruk samtidigt under en längre tid. Omfattningen av denna typ av incidenter borde kunna undvikas genom väl utformade säkerhetsstrategier som inkluderar parametrarna organisation, funktion och konsekvens för samhället. Andra incidenter kan ha inneburit att känsliga personuppgifter läckt ut. Personuppgifter som i vissa fall kan innebära liv eller död för en grupp människor som helt enkelt måste kunna förlita sig på att dessa uppgifter inte ska kunna läcka ut. I värsta fall kan konsekvenserna av denna typ få samhällets medborgare att tappa förtroendet för myndigheter och i förlängningen hota demokratin vi lever i.

Vi är väl medvetna om att problematiken vi beskriver inte har någon enkel lösning. Säkerhetsinfrastruktur blir alltmer komplex och det krävs mycket resurser, tid och ekonomiska medel för att skapa och bibehålla ett bra säkerhetsklimat i det svenska samhället. I många fall kan det, våra tidigare uppmaningar till trots, vara befogat och kanske till och med nödvändigt att välja bort flera av de kostnader arbetet med IT-säkerhet medför. Dock tycker vi, även om många företag och organisationer befinner sig i denna typ av situation, att det finns mycket som mindre, mellanstora och stora företag kan göra för att förbättra IT-säkerheten i samhället utan att det behöver medföra höga kostnader för varje enskilt företag. En diskussion om införande om rapporteringsplikt, säkerhetsstrategier för viktiga samhällsfunktioner samt ett samhällsenligt mål att förbättra säkerhetskulturen i landet tror vi skulle ha en positiv effekt på den svenska säkerhetsinfrastrukturen.

6 Vidare forskning

De undersökningar vi utfört har visat att säkerheten inte är så bra som den borde vara på svenska företag och speciellt då på de mindre. Vi har även stött på information som säger att samhällsviktiga organisationer såsom sjukhus har dålig säkerhet och även att andra större företag har brister i sin IT-säkerhet. Då de större företagen har mer att förlora på att en säkerhetsskandal inträffar kommer antagligen många utav dessa företag mörklägga incidenterna så gott de kan. Om det verkligen inträffar mörkläggning av incidenter på dem större företagen och även om dessa incidenter inte blivit mörklagda, vad skulle deras påverkan bli på samhället från ett djupare perspektiv? Vad skulle hända om företagen inte mörklägger allvarliga skandaler? Dessa frågor och funderingar hade varit intressant att forska vidare inom då man under denna uppsats fått en översikt och grund i hur säkerheten ser ut hos olika stora företag.

7 Källförteckning

7.1 Litteratur

Wilhelm, Tomas. *Professional Penetration Testing creating and operating a formal hacking lab*, Syngress, 2010

Engebretson, Patrick. *The Basics of hacking and penetration Testing Ethical hacking and penetration Testing Made Easy*, Syngress, 2011

Whitaker, Andrew. Newman, Daniel. *Penetration testing and Network Defense*, Cisco Press, 2007

7.2 Online

SecurityFocus. *SecurityFocus*, 2012
<http://www.securityfocus.com> 2012-02-20

Herzog, Peter. *OSSTMM 3 - The Open Source Security Testing Methodology Manual*, 2010
<http://www.isecom.org/mirror/OSSTMM.3.pdf> 2012-02-26

MSB. *Myndigheten för samhällsskydd och beredskap*, 2012
<http://www.msb.se> 2012-02-25

MSB. *Informationssäkerhet.se - Stöd för verksamheters informationssäkerhetsarbete*, 2010
<http://www.informationssäkerhet.se> 2012-02-26

Tieto. *Tieto på 2 minuter*, 2012
<http://www.tieto.se/om-oss/tieto-pa-2-minuter> 2012-04-17

MSB. -
incidenter, 2012
<https://www.msb.se/RibData/Filer/pdf/26170.pdf> 2012-04-17

Magnusson, Anders. *Lärdomarna efter Tieto-kraschen*, 2012
<http://www.telekomidag.se/nyheter/artikel.php?id=37469> 2012-04-17

Zirn, Tomas. *Tieto mörkade även för MSB,* 2012
<http://computersweden.idg.se/2.2683/1.434213/tieto-morkade-aven-for-msb> 2012-04-17

Cryptzone. *Oroväckande resultat om IT-säkerheten i Sverige*, 2010
<http://www.cryptzone.com/press/release.aspx?id=1392110&lang=sv&title=Oroväckande-resultat-om-IT-säkerheten-i-Sverige> 2012-05-25

Combitech. *Brister i säkerhetsberedskapen hos svenska företag*, 2011

<http://www.combitech.se/sv/om-combitech/nyheter-press-och-media/nyheter-och-pressmeddelanden/2011---12/brister-i-sakerhetsberedskapen-hos-svenska-foretag/> 2012-05-25

Combitech. *CIO Research Combitech*, 2011
<http://www.combitech.se/Documents/Bilder%20och%20filer%20sidor/Om%20combitech/Nyheter,%20press%20och%20media/Nyheter%20och%20press meddelanden/presentationCIODec%202011_final.pdf> 2012-03-20

Motorhalland. *Motorhalland,* 2012
<http://www.motorhalland.se> 2012-04-08

Widal Industri AB. *Widal Industri AB - vattenskärning, trycktankar, licenssvetsning*, 2012
<http://www.widalindustri.se/?pid=28&sub=24> 2012-05-14

Media Network. *Medianetworks.se*, 2012
<http://www.medianetwork.se> 2012-05-14

GabrielConsultingGroup. *Data Center Security Survey: Approach and Current Status*, 2011
<http://www.gabrielconsultinggroup.com/gcg-press-room-mainmenu-50/319-2011-data-center-security-survey-approach-and-current-status.html> 2012-05-25

Cryptzone. *Dataförluster på svenska företag*, 2010
<http://www.cryptzone.com/search/?q=data%20förlouster%20på%20svenska%20företag> 2012-05-24

Logica. *Mer om Logica*, 2012
<http://www.logica.se/we-are-logica/about-logica/> 2012-05-14

Holmén, *Christian. Hackerattack mot skatteverket*, 2012
<http://www.expressen.se/nyheter/hackerattack-mot-skatteverket/> 2012-05-14

Videla, Emanuel. *Hackare kom över Skatteverkets hemliga uppgifter vid intrång*, 2012
<http://computersweden.idg.se/2.2683/1.440895/hackare-kom-over-skatteverkets-hemliga-uppgifter-vid-intrang> 2012-05-14

Combitech. *Brister i säkerhetsberedskapen hos Svenska företag*, 2011
<http://www.combitech.se/sv/Om-Combitech/Nyheter-press-och-media/Nyheter-och-pressmeddelanden/2011---12/Brister-i-sakerhetsberedskapen-hos-svenska-foretag/> 2012-05-14

IDG. *Fler väljer molntjänster trots frågor om säkerhet*, 2011
<http://cloud.idg.se/2.16150/1.411389/fler-valjer-molntjanster-trots-fragor-

om-sakerhet> 2012-05-14

IT i vården. *Svenska universitetssjukhus har bristande IT-säkerhet*, 2011 <http://itivarden.idg.se/2.2898/1.392484/svenska-universitetssjukhus-har-bristande-it-sakerhet> 2012-05-14

IDG. Comhem: *Stort säkerhetshål drabbar 140 000 bredbandkunder*, 2012 <http://www.idg.se/2.1085/1.426980/comhem-stort-sakerhetshal-drabbar-140-000-bredbandskunder> 2012-05-14

Avanza bank. *Volvo står starkt*, 2006 <https://www.avanza.se/aza/press/press_article.jsp?article=5360> 2012-05-14

Mynewsdesk. *Småföretag brister i datasäkerhet*, 2010 <http://www.mynewsdesk.com/se/pressroom/it-hantverkarna/pressrelease/view/smaafoeretag-brister-i-datasaekerhet-haelften-saekerhetskopierar-aldrig-utanfoer-hemmet-466188> 2012-05-14

Symantec. *Var fjärde småföretag anser sig ha otillräcklig kunskap om IT-säkerhet*, 2007 <http://www.symantec.com/sv/se/about/news/release/article.jsp?prid=20070523_01> 2012-05-14

Aftonbladet.se. *En attack kan lamslå landet*, 2010 <http://www.aftonbladet.se/nyheter/article12535492.ab> 2012-06-02

8 Presentation av författarna

8.1 Erko Mujanovic

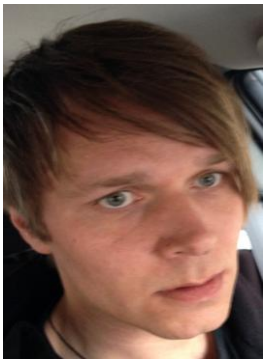
Erko Mujanovic föddes sjunde september 1989 i det forna Jugoslavien, nuvarande Montenegro. År 1992 i augusti månad flyttade han, hans två syskon och föräldrar från det då krigs härjande Jugoslavien till Sverige. Efter att ha bott åtta år i Norrköping beslutar sig familjen år 2000 att flytta till Getinge, en ort två mil norr om Halmstad där de slår sig till ro. Grundskoletiden på Getinge skolan klarar Erko av utan några större svårigheter innan han påbörjar sin gymnasiala utbildning, Teknik Entreprenörskap på Kattegatt gymnasiet i Halmstad. Sedan barnsben är Erkos stora dröm att arbeta inom Polismyndigheten och efter tre år på Kattegatt gymnasiet beslutar han sig för att ansöka till en Högskoleutbildning, valet faller då ganska självklart till den då ganska nystartade utbildningen, IT-Forensik och informationssäkerhet på Halmstad Högskola.

8.2 Frank Stehn

Frank Stehn föddes tolvte februari 1990 i Tönnersjö och flyttade sedan vidare in till Halmstad när han var åtta år. Han har studerat i grundskolorna i Eldsberga och i Trönninge. Frank har studerat IT-Teknik på John Bauer gymnasiet i Halmstad under tre år och även jobbat inom IT-support och arbetat i en IT-butik. Av intresset att lära sig mer och utveckla sin syn på hur världen ser ut inom IT

beslutade han sig att studera vidare på linjen IT-Forensik på Högskolan i Halmstad och är nöjd över sitt val av studier.

8.3 Jan-Ola Stenberg



Jan-Ola Stenberg är född 1977 och uppvuxen i Halmstad. Han har även varit bofast i Stockholm och kombinerat arbeten med studier under tiden i huvudstaden. Jan-Ola har sedan många år tillbaka ett stort datorintresse och är framför allt väldigt intresserad av IT-säkerhet. Han har samlat på sig dryga 300 högskolepoäng inom Informationsteknologi och av dessa är cirka 200 direkt säkerhetsrelaterade. Sedan flera år tillbaka driver han en egen IT-konsultfirma och har under flera år varit konsult på Försvarsmakten.