IT och Datahantering vid Börsnotering

En Analys av ett Bortglömt Område

SARA KLINGBERG

KTH Information and Communication Technology

Examensarbete inom
Kommunikationssystem
Grundnivå, 15 hp
Stockholm, Sweden

IT och Datahantering vid Börsnotering

En Analys av ett Bortglömt Område

Sara Klingberg
sarakl@kth.se

2011-09-29

Kandidatuppsats
Examinator: Professor Gerald Q. Maguire Jr.

Skolan för Informations- och kommunikationsteknologi (ICT)
Kungliga Tekniska högskolan (KTH)
Stockholm, Sverige

Tack

Först av allt vill jag börja med att tacka min examinator, Gerald Q. Maguire Jr., för alltid lika givande och värdefull handledning. Med sitt engagemang och sin breda kunskap har han bidragit med många ovärderliga råd och nya infallsvinklar.

Tack också till de två ”hemliga” VD:ar som medverkat till denna uppsats med information om deras företag, vilken jag inte hade klarat mig utan.

Jörgen Sandahl förtjänar även han ett tack för den givande intervjun, där jag lärde mig mycket om att göra affärer på Internet.

Sammanfattning

Sedan Sveriges första reglerade börs grundades 1863 har de lagar och föreskrifter som gäller börsintroduktion och handel med värdepapper till stor del anpassats efter de nya tidernas förutsättningar och behov, inte minst efter gemensamma EU-regler till följd av ökad globalisering och internationalisering. Handeln med värdepapper är också ett utav Sveriges mest reglerade områden, med stort offentligt inflytande och många kontrollverksamheter. Trots denna genomgripande reglering, både nationellt och globalt, finns en viktig del i företagsvärldens utveckling som närmast tycks ha förbisetts: IT-revolutionen.

Denna uppsats syftar till att bistå små till medelstora företag med ett antal verktyg, för att de själva ska kunna föra diskussioner kring vilka åtgärder som kan bli nödvändiga för att säkerställa lämplig hantering av IT och datasystem, då en börsnotering stundar. Fokus kommer att ligga på små till medelstora svenska företag inom *dagligvarusektorn*, vilka avser att noteras på stockholmsbörsens *Small Cap* lista.

Det finns idag endast ett fåtal lagar eller regler som rör IT och data i samband med börsnoteringar. Bland dem kan nämnas att viss information krävs på företagets hemsida samt att en loggbok skall föras över vem som delges information och när. Däremot finns tydliga krav på att information ska hanteras varsamt, vilket då också gäller digitalt lagrad sådan. I denna uppsats belyses därför en mängd säkerhetsrisker kopplade till data, digital information, samt ett antal möjliga hanteringar av dessa.

I och med att det är ett närmast orört område, men med stora möjligheter till analyser och diskussioner på djupet, men också på bredden, är det ett passande ämne för en kandidatuppsats. Området ger vidare ett utmärkt tillfälle att kombinera kunskaper inhämtade i data och IT-relaterade kurser med kunskap från kurser inom den ekonomiska disciplinen, vilket är värdefullt för min fortsatta utbildning.

Abstract

Since Sweden's first regulated stock exchange was founded, in 1863, the laws and regulations related to initial public offerings and trading of securities has largely adapted to today's conditions and needs. One obvious example of this is the adoption of common EU laws and directives, as a result of increased globalization and internationalization. Trading with securities is also one of Sweden's most regulated areas, with great public influence and many control activities. Despite this pervasive regulation, both nationally and globally, there is one important part of the business world's developments that almost seems to have been ignored: the IT revolution.

This thesis aims to assist small to medium sized businesses by illuminating a number of areas that should be discussed, regarding what measures might be necessary to ensure appropriate management of IT and computer systems, when planning an IPO. The focus will be on small to medium sized Swedish companies in the retail sector, who intends to be listed on the Stockholm Stock Exchange Small Cap list.

Today there are only a few laws or rules related to IT and data in connection with IPOs. Among them are that some information is required on the company's website and that a log has to be kept of who receive's information and when. However, there are clear requirements for information to be handled with care, which also apply to digitally stored information. Therefore, in this thesis a variety of security risks associated with data, digital information, and a number of possible management procedures for these data and information are highlighted.

The fact that this is an almost untouched area, with great potential for analysis and discussion both in depth and in breadth, makes it a suitable subject for a bachelor's thesis. The area also provides an excellent opportunity to combine the knowledge acquired in the data and IT-related courses with the knowledge from courses in the financial discipline, which is valuable for my future education.

Innehållsförteckning

Tack i
Sammanfattning ii
Abstract iii
Innehållsförteckning v
Figurförteckning vii
Akronymer och Förkortningar ix
Ordlista xi
1 Problemformulering 1
1.1 Syfte 1
1.2 Frågeformulering 2
1.3 Metod 2
1.4 Avgränsningar 2
2 Introduktion till börsnoteringar 5
2.1 Svensk värdepappershandel 5
2.2 Börsintroduktioner 6
2.3 Noteringsprocessen 7
3 Bakgrund 9
3.1 Lagar och Regler 9
3.2 Regleringar av datahantering och IT idag 9
3.3 Reglering av informationshantering 11
3.4 Introduktion till IT och datasäkerhet 12
3.5 Vad andra redan gjort 14
4 Vad ska studeras? 15
4.1 Företag 1: Livsmedelsproducent 15
4.2 Företag 2: Distributör av färdigmat 15
4.3 Jämförelse 16
5 Risk för IT-attacker 17
5.1 Lagrad data 18
5.1.1 Backup 18
5.1.2 Logiskt Intrång 19
5.1.3 Kryptering 21
5.1.4 Loggbok 22
5.1.5 Fysiskt Intrång 23

5.2 Data under överföring 24
5.2.1 Kommunikation mellan kontor/affärspartners 24
5.2.2 E-mejl 25
5.2.3 VoIP telefoni 26
5.2.4 USB-minnen och andra portabla enheter 27
5.2.5 Smartphones 27
5.3 Trådlös kommunikation 29
5.4 Tyst period vs. Transparens 29
5.5 Rutiner vid eventuellt intrång 30
6 Vem och Vad? 31
6.1 Hacker och Motiv 31
6.1.1 Hotet inifrån 32
6.2 Vad måste skyddas? 33
7 Lagring av data 35
7.1 Cloud Computing (drift i molnet) *versus* Fysisk hosting 35
7.2 Hur länge spara data? 35
8 Hemsidan 37
8.1 Finansiell information 37
8.2 Säkerhet 37
8.2.1 Allmänt 37
8.2.2 E-handel 38
9 Hur nå bättre säkerhetsrutiner? 39
10 Slutsats och Framtida Forskning 41
10.1 Lagar och krav 41
10.2 IT- och datarelaterade risker 42
10.3 Framtida Forskning 43
Referenser 45
Litteratur 45
Artiklar och rapporter 46
Lagar, Regelverk och Betänkanden 47
Avhandlingar 48
Webbsidor 48
Intervjuer 49
Appendix A 50
Appendix B 51

Figurförteckning

Figur 1, Antal Börsnoteringar, Stockholmsbörsen (Siffror från PWC: Rikspremiestudie 2011) 5
Figur 2: Ett företags informationssäkerhet (Heickerö & Larsson, 2008, s. 99) 14
Figur 3, Sannolikhet, påverkan och risk för olika smartphoneanvändare vid stöld/borttappad telefon(Från ENISAs rapport "Smartphones: Information security risks, opportunities and recommendations for users", s. 15. Pulicerad i enighet med föreskrifter) 28

Akronymer och Förkortningar

	English	Svenska
AES	Advanced Encryption Standard	
BIOS	Basic Input/Output System	
CNE	Computer Network Exploitation/Exploration	
DHCP	Dynamic Host Configuration Protocol	
DNS	Domain Name System	
DoS	Denial of Service	
DDoS	Distributed Denial of Service	
EFS	Encrypting File System	
EG	European Community	Europeiska gemenskaperna
EU	European Union	Europeiska Unionen
IDS	Intrusion Detection System	Intrångsdetekterings- och kontrollsystem
IP	Internet protocol	Internetprotokoll
IPO	Initial Public Offering	Ungefär Börsnotering
IPSec	IP-Security	IP-Säkerhet
ISO/IEC	International Organization for Standardization /International Electrotechnical Commission	
LAN	Local Area Network	
MAC	Media Access Control	
MSEK	Million (10^6) Swedish kronor	En miljon svenska kronor
NAT	Network Address Translation	
PSK	Pre-shared key	
PSTN	Public Switched Telephone Network	
PuL	Personal Data Act	Personuppgifts Lagen
QoS	Quality of Service	
SQL	Structured Query Language	
SOU		Statens Offentliga Utredningar
SCTP	Stream Control Transmission Protocol	
TCB	Transmission Control Block	
TCP	Transmission Control Protocol	
TKIP	Temporal Key Integrity Protocol	
UPS	Uninterruptable Power Supply	
VoIP	Voice Over IP	
VPN	Virtual Private Network	Virtuellt Privat Nätverk
WEP	Wire equivalent privacy	
WPA	Wi-Fi Protected Access	

Ordlista

Insiderinformation	Information om icke offentliggjord eller inte allmänt känd information, vilken är ägnad att väsentligt påverka priset på finansiella instrument (Lag 2005:377).
Aktiv attack	Data, filer eller information modifieras av obehörig (Heickerö & Larsson, 2008, s. 73).
Brandvägg	En enhet som agerar buffer mellan ett betrott och ett icke betrott nätverk.
Börsintroduktion	I Sverige definieras en börsintroduktion som ett företag som noteras på Stockholms Fondbörs i samband med en nyemission (Örtengren, 2001). En börsintroduktion i svensk mening behöver inte nödvändigtvis betyda att det erbjuds aktier till försäljning för första gången, då en tillräcklig spridning redan kan finnas. (Örtengren, 2007)
Cloud Computing	Cloud Computing innebär att all data och mjukvara hostas på en server eller serverpark, för att vid behov skickas över Internet, utan något större behov utav hårdvara (Delgado, 2010).
DoS-attack	Samlingsnamn på alla attacker som resulterar i att en tjänst inte är tillgänglig för legitima användare (Mitrovic´, 2003, s. 132).
Passiv attack	Tredje part avlyssnar eller analyserar trafik mellan två eller flera parter (Heickerö & Larsson, 2008, s. 73).
Script Kiddies	Oerfarna hackers, vilka framförallt utför attacker baserade på script de lånat av någon mer erfaren hacker. Ofta är de främst ute efter att testa scriptet, snarare än att få tag in den faktiska informationen.
IT-system	Begreppet används i texten som ett sammanfattande begrepp, vilket bland annat kan inkludera data och IT.

1 Problemformulering

Sveriges första reglerade börs, Stockholms fondbörs, grundades 1863 (nasdaqomxnordic.com, 2011). Sedan dess har mycket hänt. I mångt och mycket har de lagar och föreskrifter som gäller börsintroduktion och handel med värdepapper kommit att ständigt anpassas efter de nya tidernas förutsättningar och behov. Inte minst har de regler som gäller för svensk börshandel i stor utsträckning anpassats efter gemensamma EU-regler. I och med ökad globalisering och internationalisering har behovet av en harmoniserande värdepappershandel inom EU ökat, framförallt för att EU fullt ut ska kunna konkurrera med börserna i Asien och Nordamerika (Sandeberg, 2007). Handeln med värdepapper är inte bara ett utav de områden som är starkast influerat av EG-rätten, utan också ett utav Sveriges mest reglerade områden, med stort offentligt inflytande och omfattande reglerings- och kontrollverksamheter (Sandeberg, 2001). Trots denna genomgripande reglering, både nationellt och globalt, finns en viktig del i företagsvärldens utveckling som närmast tycks ha förbisetts: IT-revolutionen.

Information kring hur hantering av IT-system och data bör skötas lyser med sin frånvaro. Trots att varje företag av sådan storlek att det är aktuellt med börsnotering med all säkerhet äger IT-infrastruktur och enorma mängder data, vilken många gånger är känslig, finns inga tydliga riktlinjer för hur detta ska skyddas på ett acceptabelt sätt. Visserligen finns det lagar som kräver att företag säkerställer att information inte läcker ut till obehörig part, men är detta tillräckligt? Risken kan tyckas stor att företag på väg mot börsnotering inte besitter nödvändig kunskap för att förstå sitt eget behov av datasäkerhet, vilket indirekt skulle betyda att de bryter mot befintliga lagar, utan att ens veta om det, i och med kraven på säker informationshantering. Situationen blir dessutom alltmer komplex till följd av den ständigt ökande outsourcingen av IT. Inte bara låter många företag externa IT-experter sköta underhåll av hårdvara och uppdatering av mjukvara, alltfler hyr dessutom in hårdvaran som en tjänst. Det senare kallas för ”cloud computing” och får allt större utrymme på marknaden. Möjligheterna med att hyra in hårdvara, mjukvara och underhåll av dessa medför hög potential i form av effektivitetsökning och förenkling, men konsekvenserna av extern insyn i företagets mest privata delar innebär också vissa säkerhetsrisker.

Utöver säkerhetsfrågan är det även viktigt att företagets IT är kontinuerlig och inte drabbas av avbrott eller andra störningar. Även om detta inte är en lagstadgad aspekt är det inte desto mindre viktigt för företagen. Varje minut utan tillgång till webbservrar, filsystem, databaser, mejlservrar eller liknande kostar enorma mängder pengar. Längre avbrott kan få förödande effekter för företaget, i form av förlorade intäkter, minskat förtroende hos kunderna, osv.

1.1 Syfte

Denna uppsats syftar till att bistå små till medelstora företag med att belysa ett antal områden, vilka de själva ska kunna utgå ifrån då de för diskussioner kring vilka åtgärder som kan bli nödvändiga för att säkerställa lämplig hantering av IT och datasystem. Detta speciellt då en börsnotering stundar. I denna mening syftar inte lämplig IT-hantering endast på det som direkt eller indirekt uttrycks i lagtexter, utan även generella säkerhets-, effektivitets- eller stabilitetsfrågor, vilka kan appliceras på de flesta företag.

1.2 Frågeformulering

För att möjliggöra en presentation av lämpliga diskussionsområden och verktyg ämnas följande frågor besvaras:

- Vilka lagar, regler och riktlinjer finns det gällande data och IT som ett företag som skall börsnoteras måste ta hänsyn till? Då främst inom börsrätten och regelverk kring börsnoteringar.
- Hur bör företag agera för att möta de krav som finns uppsatta gällande börsnoteringar?
- Vilka andra IT- och datarelaterade risker/problem kan vara intressanta för ett företag som skall börsnoteras att fundera kring, för att på så sätt vara väl förberedda på de ökade säkerhetskraven?

För att kunna besvara frågorna ovan ställs också följande fråga:

- Hur ser behovet av IT och datahantering ut på ett företag som kan tänkas noteras på OMX Small Cap lista?

1.3 Metod

För att finna en lämplig, tänkbar IT-struktur att analysera har djupintervjuer gjorts med två mindre företag, båda i dagligvarusektorn. Det ena företaget är en livsmedelsproducent och det andra företaget är en matvaruleverantör. Gemensamt har de båda företagen ett behov av tät kundkontakt och tvingad anpassning till den omfattande regleringen som finns vid hantering av mat och dryck. Resultaten av de båda intervjuerna jämförs för att finna likheter, vilka ska komma att studeras extra noga, samt skillnader, vilka kommer diskuteras mindre, men fortfarande är av stor vikt för att få bredd på arbetet. Denna analys ligger till grund för vilka områden som senare kommer att diskuteras.

Efter att aktuella IT-områden valts ut för diskussion har dessa delats upp i lagrad data och data under överföring. Dessa diskuteras senare utifrån risk för den attack som kan tänkas aktuell, så som fysiska attacker mot lagrad data, logiska attacker mot lagrad data, attack mot data under överföring, osv. Utöver risk för attacker diskuteras dessa områden utifrån andra faktorer som kan vara av intresse ur företagssynpunkt, så som möjlighet till steglös expansion, effektivisering, hur länge data skall lagras, osv. Givetvis hanteras också den legala aspekten kring börsnoteringar, om än i många fall som en invävd del i ovan nämnda områden.

Alla ingående delar i de IT-system som diskuteras förutsätts vara svaga ur någon synpunkt. Utifrån litteratur kring datasäkerhet, rapporter, rekommendationer, avhandlingar och artiklar är dessa svagheter diskuterade.

1.4 Avgränsningar

För detta arbete kommer fokus att ligga på små till medelstora svenska företag inom dagligvarusektorn, vilka avser notera sig på NASDAQ OMX Small Cap lista. Då IT-behovet varierar från företag till företag kommer denna uppsats inte att presentera en heltäckande diskussion. Istället utgår diskussionen från ett fåtal utvalda företag, vilkas IT-behov får agera exempel.

Det finns en mängd regler rörande börsintroduktioner, insiderinformation, värdepappershandel, osv. vilka inte behandlas här, så som exempelvis förbud mot att handla med berörda värdepapper 30 dagar innan rapporter offentliggörs och förbud mot att lämna ut fingerad information till marknaden. Dock förs en kortare diskussion kring avvägningen mellan

transparens och sekretess, där behovet av IT-system vilka möjliggör hemlighållande av sekretessbelagd information fram till ett specifikt datum och därefter snabbt offentliggörande av densamma, tas upp. Överlag behandlar denna avhandling endast de områden som har en tydlig direkt eller indirekt koppling till IT och datahantering, varför områden som de ovan nämnda överlåtes till någon annan att studera.

Vad gäller IT-säkerhet och datahantering får denna uppsats ses som inspirationskälla och översikt. På varje område som nämns i denna avhandling, kan en lika lång sådan skrivas. Exempelvis kan mängder med sidor ägnas åt hur e-mejl kan skickas på ett säkert sätt, hur säkerhetskopiering utförs optimalt, osv. Uppsatsen är därför snarare ämnad att belysa de områden som bör diskuteras och ge några grundläggande verktyg att utgå ifrån i dessa diskussioner, än en fullgod lathund för hur företag bör agera och prioritera.

2 Introduktion till börsnoteringar

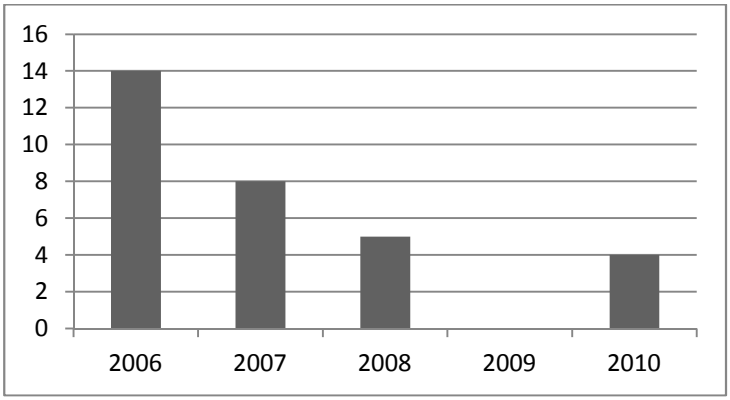
I detta avsnitt introduceras läsaren till svensk värdepappershandel, börsintroduktioner och noteringsprocessen.

2.1 Svensk värdepappershandel

Det finansiella systemet, även kallat värdepappersmarknaden, har som huvuduppgift att omfördela sparande och risk. Värdepappersmarknaden möjliggör en mötesplats för aktörer vilka önskar omfördela kapital, har behov av investeringar, krediter, riskvillighet osv. Denna marknadsplats kan delas in i aktiemarknaden, kreditmarknaden och derivatmarknaden. (Sandeberg, 2007)

För denna uppsats är det främst aktiemarknaden som är av intresse, då det är den som i första hand påverkar incitament för börsnoteringar och regleringen kring dessa. Aktiemarknaden avser handel med aktier, teckningsoptioner och konvertibler (alltså de värdepapper som företag emitterar) och har som främsta uppgift att förmedla riskkapital. Vanligen delas dess aktörer in i emittenter, investerare och börsmedlemmar. En emittent är ett företag vilket ger ut aktier och söker ägare till dessa, medan investerare är personer, företag eller institutioner som placerat/överväger att placera kapital i aktier eller andra värdepapper. Börsmedlemmar är slutligen alla de företag som förmedlar handel i värdepapper över en börs. (Sandeberg, 2001)

Till följd av bland annat globaliseringen och den därmed ökade internationella handeln, värdepappershandelns tekniska utveckling samt den låga avkastningen på traditionella sparkonton, såg aktiemarknadens betydelse en uppgång under 1990-talet och tidigt 2000-tal (Grundvall, 2004). Med detta dock inte sagt att börserna runt om i världen är på ständig uppgång. Den så kallade IT-bubblan resulterade i en djup svacka under tidigt 2000-tal, efter vilken börsen inte hunnit mycket mer än återhämta sig innan nästa finanskris stundade. Den senaste finanskrisen resulterade i ett tydligt avmattande av intresset för börsnoteringar, vilket till viss del kan ses som en indikator på inställningen till aktiemarknaden. År 2006 var antalet nynoteringar 24 stycken, därefter har det gått utför. 2010 noterades fyra nya företag på OMX och enligt en undersökning PWC låtit göra finns förhoppningar på fortsatt uppgång (PWC, 2011, s. 11). I skrivande stund är dock världsmarknaden åter i gungning och dessa prognoser har därför sannolikt ändrats.



Figur 1, Antal Börsnoteringar, Stockholmsbörsen (Siffror från PWC: Rikspremiestudie 2011)

Den svenska aktiemarknaden kan delas upp i tre delar: Börser, Auktoriserade marknadsplatser och Värdepappersinstitut/Inofficiella listor. Börser och auktoriserade marknadsplatser har båda fått särskilt tillstånd från finansinspektionen att bedriva verksamhet vilken handhar handel med finansiella instrument. Kraven gällande hur handel ska bedrivas på dessa handelsplatser, samt på företagen vilkas aktier handlas där, är både många och hårda. Dock är kraven för börser något strängare än de för auktoriserade marknadsplatser. Stockholmsbörsen är ett exempel på en börs, medan Aktie Torget är ett exempel på en auktoriserad handelsplats. Utöver dessa två handelsplatser finns också, som redan nämnts, inofficiella listor. Kraven på dessa är långt lägre än de som finns på de tidigare nämnda, både vad gäller de som erbjuder handel och företagen som handlas. En sådan lista är exempelvis First North (tidigare Nya Marknaden).(Grundvall, 2004) Då denna uppsats avser behandla börsnoteringar, är det främst faktiska börser som kommer att stå i fokus, och då i synnerhet NASDAQ OMX.

NASDAQ OMX (f.d. Stockholmsbörsen) bestod tidigare av två listor, A- och O-listan, vilka nu har ersatts med en huvudlista. Denna delas med börserna i Köpenhamn och Helsingfors. Istället för de tidigare olika listorna är huvudlistan nu indelad i tre segment, för att underlätta för investerare: Large Cap, Mid Cap och Small Cap (Örtengren, 2007). Vilket segment ett företag placeras i avgörs av dess marknadsvärde (NASDAQ OMX, 2011). De tre segmenten är vidare indelade i segment utifrån tio olika branscher: Energi, Material, Industri, Sällanköp, Dagligvaror, Hälsovård, Finans & Fastighet, IT, Telekom, och Kraft (Placera Media, 2010). I denna uppsats kommer kraven för ett företag, vilket vill notera sig på Stockholmsbörsens Small Cap studeras. Företagen som placeras i Small Cap segmentet är de med ett marknadsvärde lägre än 150 miljoner euro (swedishbankers.se, 2011). Vidare kommer speciellt fokus ligga på företag, vilka placerar sig i dagligvarusegmentet.

2.2 Börsintroduktioner

Begreppet börsintroduktion har ingen internationellt vedertagen definition, vilket medför risk för missförstånd. I Sverige definieras en börsintroduktion som ett företag som noteras på Stockholms Fondbörs i samband med en nyemission (Örtengren, 2001). Detta är inte synonymt med en IPO, vilken istället innebär det första tillfället vid vilket allmänheten erbjuds köp av aktier i ett företag. En börsintroduktion i svensk mening behöver inte nödvändigtvis betyda att det erbjuds aktier till försäljning för första gången, då en tillräcklig spridning redan kan finnas. (Örtengren, 2007)

En börsintroduktion innebär en mängd nya lagar vilka företaget måste anpassa sig efter, men också många fördelar. Det finns en stor mängd motiv för att börsintroducera ett företag. Det kanske främsta argumentet för en börsintroduktion är att genom upptagningen på en börs få tillgång till expansionskapital. Inte sällan är dock beslutet att börsnotera ett företag ett av flera alternativ för att finansiera en planerad expansion (Grundvall, 2004). Andra motiv är att få en marknadsvärdering av bolagets aktie och likviditet, ökat förtroende för bolaget och positivt tryck på företagets värdeskapande (Örtengren, 2007). De, enligt prospekten, vanligaste motiven till aktiemarknadsnotering är: Tillgång till riskkapital, apportemission (möjlighet att betala med egna aktier), nå likviditet i aktier, publicitet och status. De möjliga effekterna av en börsintroduktion är dock inte uteslutande positiva, det finns också risker med en notering. Skatteeffekterna kan bli missgynnsamma och intresse motsvarande värderingen kan vara svårt att uppnå. Vidare är processen tidskrävande och höga krav ställs på organisationen och dess

rutiner. (Grundvall, 2004) Det finns också risk för att resultat och värdetillväxt ses utifrån ett alltför kortsiktigt perspektiv (Örtengren, 2007).

För att få noteras på någon av Sveriges börser måste företaget uppfylla en mängd krav. Dessa noteringskrav är uppdelade i krav inför noteringen och fortlöpande krav (dock måste även de fortlöpande kraven vara uppfyllda redan innan noteringen sker, för att denna ska godkännas). (Grundvall, 2004). I nästföljande avsnitt, ”noteringsprocessen”, behandlas de regler som företag måste följa och de krav som måste uppfyllas innan ett företag tillåts noteras på börsen. Senare, i avsnittet om ”lagar och regler” behandlas de krav som företaget förväntas följa kontinuerligt, även efter det att introduktionen genomförts.

2.3 Noteringsprocessen

Innan ett företag accepteras till börsen måste det genomgå en legal granskning. Denna utförs först av en extern advokat och granskas sedan av börsrevisorn och NASDAQ OMX. Börsen håller också utbildningar för företagsledare, styrelsemedlemmar och personal, där de utbildas gällande bland annat noteringskrav, noteringsavtalet och insiderfrågor. Bland de övriga kraven finns exempelvis lägsta tillåtna aktiepris, historik, dokumenterad vinstintjäningsförmåga och krav på prospekt. (Grundvall, 2004) Prospektet är ett viktigt instrument i och med att det är detta som levererar den information som ska ligga till grund för investerares beslutsfattning (Sandeberg, 2001). Noteringsprocessen kan se lite olika ut beroende på företag. Ett flertal moment är dock ofta gemensamma. Nedan följer en översikt över en typisk noteringsprocess (Grundvall, 2007):

1. Övervägande av olika alternativ – planering, beslut
2. Anpassning och översyn/komplettering av:
    a. Styrelse, styrelsearbete
    b. Affärsplan, affärsmodell
    c. Organisation och ledning
    d. Styrsystem och intern kontroll
    e. Bolagsordning
    f. Ägarstruktur
    g. Extern Informationsgivning
    h. Intern informationsgivning
3. Kontakt tas med rådgivare (bank, värdepappersinstitut, revisor)
4. Besök på börsen, vilken utser revisor för undersökning
5. Prospektarbete
6. Aktiemarknadsutbildning av styrelse, revisorer, företagsledning och personal
7. Bolagskommittébeslut
8. Distribution av prospekt och spridning av aktier
9. Noteringsavtal och notering
10. Löpande informationsgivning, kontakt med analytiker m.fl.
11. Ettårsuppföljning

Processen är tidskrävande och bör därför påbörjas långt innan förtaget avses börssättas. För att processen inte ska bli alltför svår och långdragen tar företag ofta in extern expertishjälp. Denna kan exempelvis bestå av finansiella och/eller legala rådgivare (Örtengren, 2007). Börsen ställer visserligen inga krav på extern specialisthjälp, men de inte sällan snåriga regelverken

medför behov av specialkompetens på vissa områden, vilket företaget allt som oftast inte besitter.

3 Bakgrund

Detta avsnitt behandlar de förutsättningar som ligger till grund för det kommande arbetet, i form av lagar och regler, framförallt med betoning på IT, datahantering och informationshantering. Avslutningsvis ges en introduktion till datasäkerhet.

3.1 Lagar och Regler

En förutsättning för att värdepappersmarknaden ska fungera är gemensamma lagar och regler. Värdepappersmarknaden är en utav de mest reglerade marknaderna, med stort offentligt inflytande och omfattande reglerings- och kontrollverksamheter (Sandeberg, 2001). De viktigaste lagarna för den svenska aktiemarknaden är den lag som behandlar börsverksamheten, lagen om värdepappersrörelse och den om kontoföring av finansiella instrument. Som komplement till dessa finns också föreskrifter, rekommendationer och avtal, vilka i mer detalj anger hur marknaden ska bedrivas. Den ökade internationaliseringen bidrar till ökad efterfrågan på gemensamma regler och riktlinjer.(Grundvall, 2004) Redan sedan tidigare är regleringen kring värdepappersmarknadsområdet starkt influerad av EG-rätten (SOU 2006:50), men det omfattande arbetet inom EU för att öka harmoniseringen mellan unionens olika värdepappersmarknader är ännu i full gång. Nya direktiv och förordningar antas årligen, vilka för unionens länder närmare varandra vad gäller värdepappershandel.

För att marknaden och dess prissättning ska fungera på ett effektivt och korrekt sätt är det av yttersta vikt att allmänheten känner förtroende för systemet. Detta förtroende är i stor utsträckning beroende av delgivningen av korrekt information, då det är denna som ligger till grund för investerares beslut. Informationen måste vara väsentlig, snabb och spridas till alla aktörer samtidigt för rättvisande prissättning, varför det är viktigt att företaget sammanställer en informationspolicy.(Grundvall, 2004) I denna ska bland annat vem som är talesman för företaget ska framgå, vad som i regel ska offentliggöras, hur och när offentliggörande skall ske, informationshantering vid kris samt aktiemarknadens krav på information (NASDAQ OMX, 2011). För att följa denna policy måste företaget ha tillgång till system för löpande rapportering (Grundvall, 2004).

Bland de fortlöpande kraven betonas också bland annat vikten av börserfarenhet och lämplighet bland styrelsen och ledningen. Företaget måste vidare uppfylla krav ställda på ledning och ekonomistyrning med avseende på informationsgivning till aktiemarknaden. Snabba, tillförlitliga rapporter ska finnas att tillgå, samt analyser av dessa. Det finns också krav på hur företagets hemsida ska fungera och vara utformad. På hemsidan ska all offentliggjord information finnas att tillgå, och denna ska gå tillbaka minst tre år i tiden. Även aktuell bolagsordning ska finnas tillgänglig på hemsidan. (Grundvall, 2004)

Bland de specialverksamheter vilka måste lämna ytterligare information (exempelvis fastighetsbolag och rederier) finns inte företag kopplade till dagligvaruhandel med (Finansinspektionen, 2011), varför dessa specialregler inte hanteras i denna rapport.

3.2 Regleringar av datahantering och IT idag

Att finna information angående hur data och IT-system bör hanteras i samband med och efter en börsintroduktion har visat sig vara svårt. På enstaka platser nämns data och/eller IT-system som i förbifarten, men aldrig förs någon djupare diskussion eller presenteras några användbara rekommendationer eller krav. Då en börs enligt lagen ska ha tydliga och öppet

redovisade regler för upptagande av ett företag till handel på reglerad marknad (lag 2007:528), är den bristande informationen kring data och IT-krav sannolikt ett tecken på sådana inte finns. I den så kallade ”prospektförordningen” finns listor över vad som måste ingå i ett prospekt, där data och IT helt saknar utrymme. Vidare uttrycker förordningen att det inte är tillåtet för en myndighet att kräva att viss information ska ingå i prospektet, om denna inte efterfrågats i förordningen (Kommissionens Förordning (EG) 809/2004). Undantaget är om emittenten har en komplex finansiell historia, då viss finansiell information kan krävas in (Kommissionens förordning EG 211/2007). Därmed alltså sagt att det inte finns något krav på att nämna data eller IT i prospektet. Dock kan det vara en god idé att ändå säkerställa en trygg hantering av IT- och datasystem, för att inte indirekt bryta mot existerande lagstiftning, gällande exempelvis informationshantering.

Under punkt två, Anpassning och översyn/komplettering, i noteringsprocessen som presenterades tidigare, ingår att anpassa förtaget efter de insiderregler som finns. Även om det inte uttryckligen nämns något om hur osäkert hanterad data och insiderbrott är sammankopplade är det inte svårt att själv dra paralleller. Exempelvis kan ett företag med bristande säkerhetsrutiner ha ”missat” att lägga in behörighet för access till viss, företagskänslig data, vilket möjliggör för alla anställda att komma åt denna, istället för endast de få som egentligen bör vara insatta. En till synes trivial miss som denna kan leda till att en anställd inom företaget kan läcka känslig information till utomstående part, utan att ge möjlighet för företaget att spåra läckan. Detta är bara ett av många insiderrelaterade brott som är kopplat till hanteringen av IT- och datasystem.

Den börsrevisor som utsetts av börsen för att granska företaget riktar främst in sig på organisation och styrsystem, extern informationsgivning och finansiell ställning, resultatutveckling och finansiering. I detta ingår bland annat att bedöma verksamhetens IT-beroende och hur detta hanteras. Dock görs ingen detaljerad analys, utan endast övergripande. (Grundvall, 2004) Vad som menas med verksamhetens IT-beroende förklaras emellertid inte närmare, varken i Grundvalls text, i OMX regelverk för emittenter, de lagar som berör värdepappershandel eller någon annan stans. Detta ger utrymme för egna antaganden och spekulationer. Förmodligen ligger fokus på att säkerställa att företagets IT-behov tillgodoses, även vid eventuellt missöde, så som förlorad internetanslutning, brand, osv. Vidare bör företaget säkerställa att ekonomi och förutsättningar finns för att på ett smidigt sätt utöka IT-systemet då minne eller liknande tar slut, eller vid eventuell expansion av företaget.

Som del i prospektet, vilket är en obligatorisk del av noteringsprocessen, ska företagets riskfaktorer tas upp. Dessa delas upp i faktorer kopplade till emittenten och faktorer kopplade till värdepappret (Finansinspektionen, 2011). En tvivelaktig datahantering kan få förödande konsekvenser för företaget, varför detta borde behandlas under denna punkt. Dock finns inga krav eller riktlinjer gällande huruvida det är lämpligt att diskutera denna typ av fråga inom riskområdet.

Det enda i regelväg gällande data och IT som finns på pränt på ett flertal ställen är utformningen av hemsidan, men då främst i informationsgivningshänseende. All offentliggjord information ska finnas tillgänglig på hemsidan, precis som aktuell bolagsordning. Offentliggjord information ska finnas tillgänglig i minst tre år, medan finansiella rapporter ska finnas tillgängliga i minst fem år. Även bolagets kalender, vilken visar uppgifter om viktiga datum för offentliggörande av finansiell information, datum för årsstämma, osv. bör finnas på hemsidan.

(NASDAQ OMX, 2011) I samband med börsintroduktion måste också prospektet offentliggöras på hemsidan (Lag 1991:980).

Då information i stor utsträckning är synonymt med data i dagens företagsmiljöer bör all data som berör företaget hanteras på sådant sätt att de föreskrifter som finns för informationshantering och för att förhindra insiderläckage följs. För denna uppsats är det således inte regler för IT- och datahantering som ligger till grund för kommande diskussioner (då sådana inte finns), utan regler och krav för insiderbrott och hantering av information.

3.3 Reglering av informationshantering

Möjligheten till notering beror till stor del på företagets förväntade förmåga att klara kraven gällande offentliggörande av finansiell och annan kurspåverkande information (NASDAQ OMX, 2001). Efter varje räkenskapsår ska företaget offentliggöra årsredovisning och eventuell koncernredovisning. Dessutom ska en halvårsrapport offentliggöras efter räkenskapsårets första sex månader och delårsredogörelse eller kvartalsrapporter där emellan (lag 2007:528). Innan dessa offentliggöranden är det av yttersta vikt att ingen obehörig får tillgång till rapporternas information, då detta kan skapa spekulationer och leda till felaktiga aktiekurser och då dubiösa personer kan dra nytta av den icke offentliggjorda informationen och på så sätt göra olagliga aktievinster. När rapporterna är redo att offentliggöras är det dock viktigt att detta görs snabbt och effektivt, för att handeln ska ske så rättvist som möjligt. (NASDAQ OMX, 2011) Denna ständiga slitning mellan sekretess och transparens är en utmaning för börsnoterade företag (Finansinspektionen, 2011). Lagstiftningens höga krav på diskretion och sekretess i kombination med förväntad transparens och öppenhet är något av en paradox, vilken ställer höga krav på företaget. Lagarna måste följas utan att resultera i förtroendekriser till följd av bristande kommunikation. I och med att denna problematik är ständigt återkommande bör tydliga rutiner instiftas, vilka kan möjliggöra mer friktionsfri hantering. Det bör finnas ett styrsystem som anger regler och strategier och företagen bör ”öva sig” på att ta fram ekonomiska rapporter redan innan börsintroduktionen (Lindholm, 2002).

För att säkerställa att endast behöriga personer får tillgång till företagskänslig information och att denna information inte används på felaktigt sätt, måste alla börsnoterade företag föra loggbok. Denna har till syfte att göra emittenten uppmärksam på vilka anställda som får ta del av kurskänslig information och när denna delgivning sker (Finansinspektionen, 2007a). Vad som ska anges i loggboken är: skäl till att personen finns med, när denne fick tillgång till informationen (gärna med klockslag) och senaste tidpunkten då förteckningen uppdaterades (Finansinspektionen, 2007b). Om känslig information ändå skulle läcka ut är det viktigt att företaget har etablerade rutiner för att omedelbart överlämna utläckt information till börsen samt offentliggöra denna (lag 2007:528).

I de rutiner gällande informationshantering som ska finnas på plats i god tid före planerad börsintroduktion ingår också system och procedurer för finansiell rapportering. Organisationen ska möjliggöra snabb spridning av information, så snart den offentliggjorts. Ekonomisystemet ska snabbt kunna leverera tillförlitliga rapporter och annat nödvändigt beslutsunderlag till ledning och styrelse. Även de delårs- och bokslutsrapporter som nämns ovan skall levereras snabbt och tillförlitligt. (NASDAQ OMX, 2011) Emittenten ska enligt lag fortlöpande informera börsen om sin verksamhet och offentliggöra de upplysningar kring verksamhet och värdepapper som kan tänkas vara av betydelse för kursvärdet (lag 2007:528). Vidare ska ett dokument, som

innehåller eller hänvisar till all information företaget offentliggjort senaste tolv månaderna, ges ut årligen (Europaparlamentets och rådets direktiv 2003/71/EG).

Några exempel på situationer då informationsplikt kan föreligga är vid order- och investeringsbeslut, pris- och valutaförändringar, inledande eller uppgörelse av legala tvister samt relevanta domstolsbeslut, myndighetsbeslut, finansiella svårigheter, osv. (NASDAQ OMX, 2011)

3.4 Introduktion till IT och datasäkerhet

Att informationshantering är en kritisk del av kraven inför en börsnotering har redan framgått. Företagsinformation så som beställningar, kontakter, leverantörer, fakturor, kundinformation osv. är viktiga tillgångar för företaget, vilka måste skyddas från konkurrenter och felaktig borttagning (hp.com, 2011). Det är i börsrätten tydligt fokus på att i den mån det går eliminera risk för att känslig information läcker ut till obehörig part, vilket kan leda till insiderbrott. Den som innehar insiderinformation får inte agera på värdepappersmarknaden utifrån denna, varken för egen eller för någon annans räkning. Inte heller får denna insiderinformation spridas vidare till obehörig part eller ligga till grund för en uppmuntran till någon annan, med avsikt att få denne att agera genom att förvärva eller avyttra finansiella instrument. (Lag 2005:377). Information ska av företag behandlas som en viktig tillgång, vilken ska skyddas precis som organisationens övriga tillgångar. Informationssäkerhet handlar således om att skydda all form av information, oavsett format.

Om Ett företags informationssäkerhet (Heickerö & Larsson, 2008, s. 99) innefattar företagets sammanlagda information, handlar IT-säkerhet istället om att skydda den del av informationen som är utav elektronisk form, så som exempelvis e-post, webbsidor och andra elektroniskt lagrade filer. (Mitrovic´, 2003, s. 27-28) Som redan klargjorts är det just IT-säkerheten som är i fokus i denna avhandling. Men frågan är då hur ett företag säkerställer tillfredsställande hantering av elektronisk information, både vad gäller fysiska och logiska hot. Vidare måste både lagrad information och sådan under överföring skyddas. Fortsättningsvis kommer data och information användas synonymt, där all typ av information som kan lagras elektroniskt kommer att åsyftas.

Det finns tre egenskaper som utgör grunden för IT-säkerhet (Mitrovic´, 2003, s. 28):

Sekretess	Att ej avslöja datainnehåll till obehörig part, varken avsiktligt eller oavsiktligt
Integritet	Säkerställa att obehörig part inte kan modifiera datainnehåll och att innehållet är konsistent
Tillgänglighet	Åtkomsten till ett system ska vara pålitlig för den som är behörig.

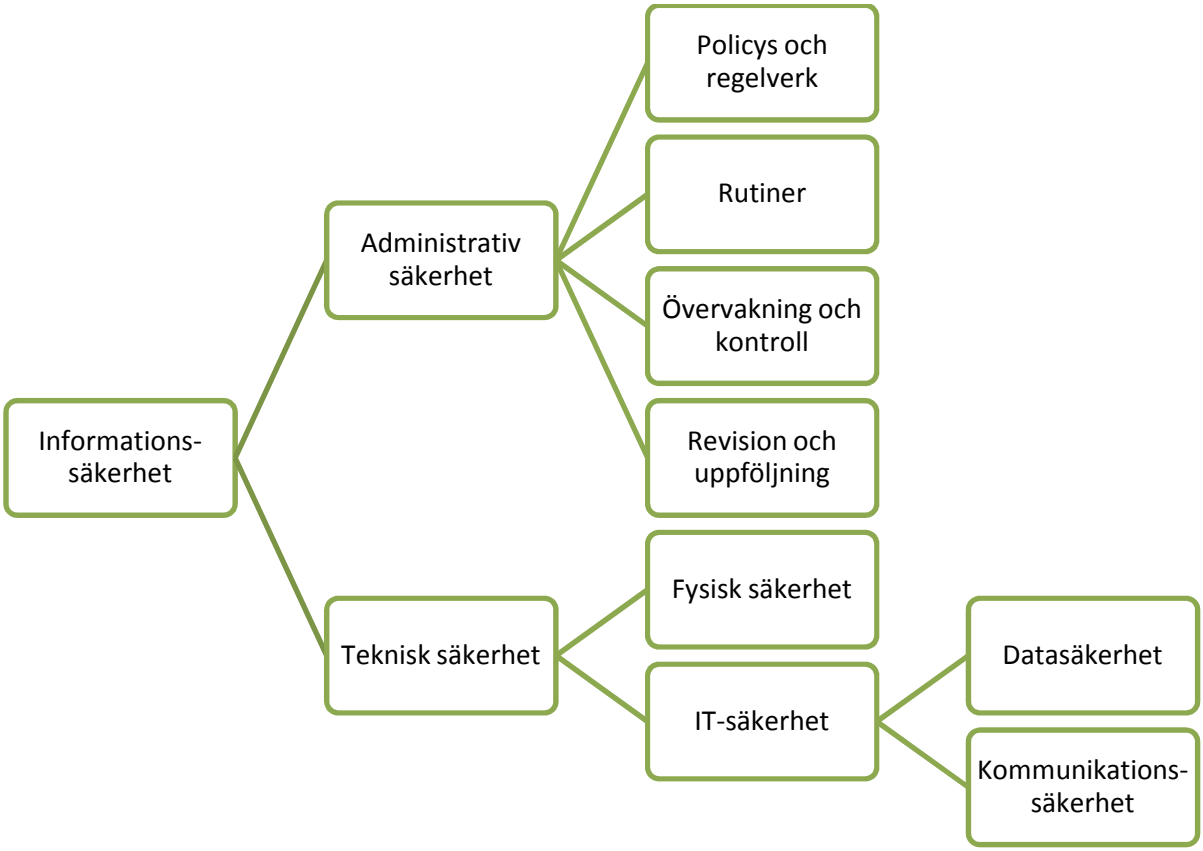
Det finns idag inget fungerande skydd vilket kan täcka in alla dessa områden, utan istället många olika sådana med egna specialiteter och inriktningar. För att nå hög säkerhet krävs således mer än ett skydd. Det mest lämpliga är vanligtvis att använda flera lager av säkerhetslösningar (Crume, 2000, s. 15). Denna flerlagersprincip, ibland kallad lökmetoden, är ett effektivt sätt att skydda sig mot IT-attacker. Den bygger på att attacken försvåras genom ett flertal sammankopplade lager som hanterar informationssäkerhet. För att komplettera tekniken krävs intrångsdetektering och kontroll av de personer som har tillgång till den lagrade informationen (Heickerö & Larsson, 2008, s. 109). Det är dock viktigt att ha förståelse för att lökmetoden och dess ingående delar (vilka väljs av företaget) inte på något sätt är en garanti för

att företaget ska undgå att drabbas av attacker eller andra intrång. När det kommer till säkerhetsdiskussioner bör det därför talas i relativa termer. I praktiken är ingen lösning helt ogenomtränglig, varför diskussionen bör handla om ifall alternativ X är säkrare än alternativ Y, snarare än huruvida alternativ X är säkert eller inte (Crume, 2000, s. 11-12). Det mest effektiva sättet att skydda hemlig information är dock att helt frikoppla en dator eller ett nätverk från Internet.

Det går allt som oftast att finna ett säkrare alternativ än det företaget har idag, men ett sådant alternativ behöver inte nödvändigtvis vara attraktivt för företaget. Högre säkerhet resulterar ofta i mer komplexa system och lägre användarvänlighet. Det svåra är således ofta att hitta en balans mellan smidighet och säkerhet. Då mer avancerad teknik vanligtvis finns att tillgå är det sällan en rent teknisk fråga, utan snarare en affärsfråga (Crume, 2000, s. 14). Även balansen mellan riskhantering och möjlighet måste övervägas. Överdriven rädsla för möjliga risker kan kväva hela verksamheten. Att istället ignorera riskerna och ge utrymme för möjligheter kan givetvis få förödande konsekvenser. För att finna en passande risknivå är det lämpligt att först och främst ta fram en riskanalys, gärna innan företaget drabbas av ett intrång (Crume, 2000, s. 39-40) Riskanalysen bör bland annat innehålla följande diskussionsområden (Crume, 2000, s. 42-43):

- *Vilka resurser bör skyddas*? Kategorisera dessa i grupper
- *Vad/Vem bör data skyddas ifrån*? Det kan exempelvis handla om konkurrenter, så kallade ”script kiddies”, politiska aktivister, missnöjda anställda, osv.
- *Vad blir kostnaden för eventuellt intrång*? Kan gälla exempelvis rykte, effekt av förlorad data, minskat kundförtroende osv.
- *Vad kostar det skydd som behövs*? En nyckelregel är att inte betala mer än vad informationen som avses skyddas är värd
- *Vad är sannolikheten för att intrång sker?* Detta är givetvis endast en uppskattning.

Sammanfattningsvis kan sägas, att det för att ett företag ska kunna nå en säker IT-miljö krävs att tre element alla är effektiva och säkra: verktyg, människor och policys. (Crume, 2000, s. 62) Alla dessa områden kommer att hanteras i uppsatsen, då det är av yttersta vikt att de både var och ett för sig, men framförallt som helhet, hanteras på ett säkert och tillfredsställande sätt. I denna uppsats kommer inledningsvis verktygen att diskuteras. *Vilka alternativ finns för att skydda företagets IT?* Därefter kommer den mänskliga faktorn att behandlas. *Vem kan tänkas göra intrång? Och varför?* Avslutningsvis kommer en diskussion kring *hur företaget når bättre säkerhetsrutiner* föras.



Figur 2: Ett företags informationssäkerhet (Heickerö & Larsson, 2008, s. 99)

3.5 Vad andra redan gjort

Det är inte bara i lagböcker och regelverk som IT och datahantering i samband med börsnoteringar lyser med sin frånvaro, inte heller har det gått att finna rapporter, avhandlingar eller liknande, vilka belyser denna problematik. Med största sannolikhet finns ett antal konsultbyråer vilka genomför analyser av företags infrastruktur och datahantering inför börsintroduktioner, men de delar inte med sig av sina lärdomar och avprickningslistor till allmänheten. Vad det har visat sig finnas bättre tillgång på är avhandlingar om informationshantering. Dessvärre har ingen av de hittills lästa behandlat eller ens vidrört dataområdet, men en god tillgång till informationshanteringsidéer medför ändå att de mest grundläggande tankarna och förutsättningarna inte måste tas fram på nytt i denna avhandling. Det finns även ett antal rapporter och böcker om själva noteringsprocessen, men i och med den bristande IT-regleringen i denna fas är dessa inte av nämnvärd betydelse för arbetet.

Poängteras skall dock att den sökning bland både lagar och uppsatser som gjorts, till största del begränsats till Sverige. Det är mycket möjligt att utländska aktörer, myndigheter eller studenter gjort en undersökning motsvarande den som avses göra här, men då lagstiftningen kan se mycket olika ut från land till land har de utländska källorna valts bort.

Dessbättre tycks det finnas mängder av litteratur och rapporter för respektive data/IT-problematik. Idéer och lösningar från sådana källor används genom hela rapporten, men presenteras på sina respektive platser snarare än här.

4 Vad ska studeras?

För att säkerställa att rätt komponenter och problematik analyseras och diskuteras i detta arbete är (som tidigare nämnts) intervjuer genomförda med två olika företag. Båda företagen önskar vara anonyma, då ingen av dem ännu genomfört en börsintroduktion, varför de här endast omnämns som *Företag 1* och *Företag 2*. De båda företagen är av relativt olika natur, men med förvånansvärt många gemensamma nämnare i fråga om IT-behov inom organisationen. Nedan följer en kortare beskrivning av de båda företagen, följt av respektive företags IT-situation och avslutningsvis en jämförelse av dessa. De behov som nämns nedan är i de flesta fall redan uppfyllda och företagen önskar således ha rätt förutsättningar för att kunna bevara dessa IT-system. Ett fåtal punkter är istället sådant som företagen önskar av framtiden.

4.1 Företag 1: Livsmedelsproducent

Företaget är en livsmedelsproducent, med en omsättning på ca 100 MSEK. Produktionen ligger i en medelstor stad i Sverige, men huvudkontoret är placerad på annan ort. Utöver tillverkningsplats och huvudkontor finns också ett antal mindre kontor i Sverige, samt ett antal anställda utanför Sveriges gränser.

Företaget har idag lagt ut stora delar av sin IT-drift på entreprenad, men äger fortfarande hårdvaran själva. I stora drag har företaget behov av följande:

- Fillagring
- Databas med kunddata
- Databas med produktdata
- Ekonomisystem (inklusive lagersystem)
- Säkerhet i samband med e-mejlkommunikation
- Säkerhet IP-telefoni
- Backup
- Skydd mot virus/intrång
- System för fjärråtkomst (både inom Sverige och utanför)
- Säker kommunikation med serverhall
- Möjlighet att expandera
- Planer på införande av trådlöst nätverk
- Hemsida:
  - Försäljning
  - Marknadsinformation
  - Finansiell information

4.2 Företag 2: Distributör av färdigmat

Företaget är en mellanhand mellan konsumenten och restaurangen, med en omsättning på ca 50 MSEK. Företaget levererar färdiga maträtter till kunder på ett par andra orter i Skandinavien. De har ingen egen produktion, utan sammanför istället kundstock, restauranger samt budfirmor. De flesta anställda befinner sig i Stockholm, men nätverket måste regelbundet kunna nås från andra orter i Sverige, och ibland även från utanför landets gränser.

Företaget har idag lagt hela sin IT-drift på entreprenad, vilken hostar hela systemet i molnet. Övergripande kan företaget sägas behöva:

- Fillagring
- Databas med kunddata
- Databas vilken hanterar speciella rabatter/kampanjer
- Databas för leverantörer/logistik
- Ekonomisystem
- Säkerhet i samband med e-mejlkommunikation
- Säker IP-telefoni
- Backup (både lokalt för test av utveckling, samt i serverhallen)
- Skydd mot virus/intrång
- System för fjärråtkomst (både inom Sverige och utanför)
- Säker kommunikation med serverhall
- Möjlighet att expandera
- Planer på införande av trådlöst nätverk
- Hemsida:
  - Försäljning
  - Information

4.3 Jämförelse

Trots att det ena företaget är producerande, medan det andra endast förmedlar en tjänst, är deras behov slående lika. Detta resultat kan antas betyda att det är ett antal nyckelfaktorer vilka är kritiska för närmast alla företag. Dessa kommer alla att diskuteras i denna avhandling. Den enda större skillnaderna mellan de båda företagen är att det ena äger sin egen hårdvara i form av servrar, medans det andra lagt ut sin serverhållning på entreprenad, samt innehållet i databaserna. Då själva innehållet i databaserna inte kommer att diskuteras närmare i denna avhandling, utan istället hur data placerat på en server (i detta fall kund-/logistik-/produktdata placerat på en databasserver) skyddas, får det båda företagen ses bidra med en gemensam grund för det fortsatta arbetet. Vad gäller de observerade serverskillnaderna kommer fördelarna och nackdelarna med att placera servrar i molnet att behandlas.

5 Risk för IT-attacker

Insiderinformation behöver inte nödvändigtvis hamna i fel händer för att en anställd eller annan behörig person spridit denna vidare. Det finns också viss risk att en obehörig person tillgodogör sig denna information på egen hand. I det moderna IT samhället kan detta handla om fysiska inbrott där inkräktaren stjäl exempelvis laptops, men också om professionella så kallade ”datahackers”, som lägger beslag på information genom att ta sig igenom ett företags säkerhetssystem och olovligen tillgodogöra sig data. Det är därför viktigt att företag är medvetna om vilka risker som finns kring datahantering och anpassar systemen därefter. Dataintrång innebär att utan tillstånd bereda sig själv tillgång till, ändra, förstöra, blockera eller registerföra uppgifter som är avsedda för automatisk behandling (Brottsbalk 1962:700). I detta avsnitt kommer dock även andra typer av brott och risker relaterade till data och IT att behandlas, så som brotten ”brytande av post- och telehemlighet” (vad gäller e-mejl) och ”intrång i förvar” (serverhallar, förvaring av bärbara datorer, osv.), vilka båda prioriteras framför paragrafen om dataintrång, vilken alltså inte gäller om någon av ovanstående är applicerbara. För att inte begränsas till dataintrång används här begreppet ”IT-attack” som samlingsnamn. En IT-attack kan innefatta alltifrån trafikövervakning till förstöring av utrustning. Sådana attacker kan vara aktiva eller passiva. (Heickerö & Larsson, 2008, s. 72-73). Några exempel på IT-attacker är följande (Heickerö & Larsson, 2008, s. 73):

- Dataintrång med avsikt att etablera kontakt med komponenter och utrustning
- Påverka systemens stabilitet och säkerhet genom induktion av skadlig kod
- Störning av trafik och skapandet av felfunktioner
- Överlastningsattacker, Denial of Service (DoS) och spamming
- Övertagande av utrustning genom användning av skadlig eller direkt hacking
- Vilseledning – deception
- Plantering och manipulering av information – influence
- Avlyssning av trafik – sniffing
- Förstöring av hela eller delar av systemet

Inledningsvis kan det vara värdefullt att grundläggande kunskap kring skadlig kod och attacker. Det finns flera typer av skadlig kod (”malware”). *Virus* är reproducerande kod, vilken behöver ett värdprogram för att föröka sig. Ett virus kopierar sig själv och sprider sig vidare i systemet. Virus kan bland annat ha som syfte att förstöra data och skapa minnesförluster. En annan typ av skadlig kod är *maskar*, vilka också de förökar sig själva, men utan behov av värdprogram. Istället utnyttjar de säkerhetshål i operativsystemet. *Trojaner* är kod som inte reproduceras, men är minst lika skadlig. Trojaner gömmer sig i till synes hederliga program och syftar till att stjäla eller förstöra data, eller låna processortid. Exempelvis kan en trojan användas för att logga användarnamn och lösenord, vilket kan möjliggöra för en hackare att senare få tillgång till ett system. (Heickerö & Larsson, 2008, s. 75).

Attacker kan delas in utifrån de effekter de resulterar i: Fysiska effekter, Syntaxeffekter och Semantiska effekter. Då en part utsätts för en överbelastningsattack (DoS-attack) kan verksamheten inte bedrivas optimalt, i och med att tjänster inte kan utnyttjas korrekt, detta räknas som en *fysisk effekt* av förstöring av informationsstruktur. *Syntaxeffekter* är istället sådana som orsakats av attacker med syfte att sabotera logiken i systemet, genom exempelvis inducering av virus, trojaner, trafikavlyssning och hackning. Detta kan skapa fördröjning av information eller oberäkneliga beteenden. Slutligen finns det semantiska effekter, vilka ämnar

förstöra förtroendet för systemet och informationen. Information förvanskas eller manipuleras då, vilket vilseleder intressenter.(Heickerö & Larsson, 2008, s. 34).

5.1 Lagrad data

Lagrad data innebär all data som finns lagrad i någon form, på lokala hårddiskar, servrar, etc. Data som är lagrad är utsatt för andra typer av hot än den under överföring och kräver därför egna säkerhetsdiskussioner. I detta avsnitt hanteras sådana frågor, så som exempelvis behovet och hanteringen av backup och intrång, såväl logiskt som fysiskt.

5.1.1 Backup

Hela 40 % av alla små till medelstora företag genomför ingen backup alls. Detta är ytterst skrämmande då 90 % av de företag som förlorar all dess data lägger ner sin verksamhet inom ett år (Tandberg Data, 2010, s. 3). Data är företagets livsnerv och bör därför behandlas med varsamhet. Lämpligen bör företag kombinera backup och arkivering, där backup kan sägas användas för kortsiktigt skydd och arkivering för långsiktigt (Tandberg Data, 2010, s. 3). Arkivering mögliggör lagring av data för flera decennier, vilket är nödvändigt för många företag, dels av lagstadgade skäl, dels då långvarig lagring kan behövas för att kunna kvalitetssäkra och tillvarata kundkontakter. För arkivering kan exempelvis band användas, då det är billigt och tillförlitligt (Tandberg Data, 2010, s. 4). Dock kräver det att arkiverade data inte behöver kommas åt regelbundet, så band är relativt långsamma. Varje företag borde också ha ett schema för all data som ska bevaras. Ett sådant schema tar dels hänsyn till de legala och organisationella krav som finns, dels beskriver det hur länge data ska bevaras och hur den bör hanteras då den inte längre behövs. För att kunna ta fram ett bevarandeschema måste företaget besluta kring vilken data som ska arkiveras och vilken det ska tas backup på. All data måste också klassificeras för att säkerställa att rätt krav tas hänsyn till. (Tandberg Data, 2010, s. 4). Efter att det beslutats om vilken säkerhetsklass data skall ha samt huruvida den skall arkiveras eller tas backup på, måste det också beslutas hur ofta denna säkerhetskopiering skall ske. För att fatta beslut kring detta är det lämpligt att fundera kring hur ofta data ändras samt hur mycket data företaget har råd att förlora utan att företaget drabbas alltför hårt. För många företag fungerar det att ta backup på nya och ändrade filer dagligen, och för alla filer veckovis. Dock kan det vara aktuellt att ta backup av kritiska filer flera gånger dagligen. (Tandberg Data, 2010, s. 4). Att endast ta backup på filer som lagts till eller ändrats sedan senaste backupen kallas partiell backup. Partiell backup kan vidare delas in i inkrementell och differentiell backup, där båda innebär att en full backup görs sällan men i det först nämnda fallet görs backup av filer som ändrats sedan senaste backupen (oavsett om den var en full eller partiell backup) mer ofta. Differentiell backup innebär istället att den partiella backupen görs endast på filer som ändrats sedan den senaste fullständiga backupen. Inkrementell backup har fördelen att säkerhetskopieringen går snabbare, men till kostnad av långsammare återställningstid vid eventuellt haveri. Motsatt gäller för differentiell backup. Det är således av intresse för varje företag att bedöma vilken av dessa två metoder som passar den egna verksamheten bäst. Ett företag som inte har råd med att systemet ligger nere en sekund för länge bör välja differentiell backup. Om det istället är kostnadsminimering i form av hårdvara som är prioriterad bör inkrementell backup väljas, då denna kan kräva färre lagringsband. (Tandberg Data, 2010, s. 5).

Data lagrad på en hårddisk kan försvinna eller förstöras av en mängd orsaker. Hårdvaran kan slitas ut, en vattenläcka förstöra den, en anställd oavsiktligt radera data, osv. Ett sätt att möjliggöra återställning efter en hårddiskkrasch är att ständigt säkerhetskopiera information.

Som minimikrav bör företaget sätta upp att all programvara ska vara skyddad med hjälp av säkerhetskopiering. Systemdata bör kopieras minst en gång per månad och användardata bör kopieras dagligen. (Mitrovic´, 2003, s. 110). Lämpligen ska det som ej på ett enkelt sätt kan återställas säkerhetskopieras. Enskilda användare kan själva få välja ut vad de behöver säkerhetskopiera och placera detta i en specifik mapp. Då företaget förlorar enorma mängder pengar om exempelvis hela filservern går ner och ingen i personalen därmed kan arbeta, är det av yttersta vikt att de servrar som påverkar hela personalstyrkan skyddas extra noga. För att vara säkra på att säkerhetskopiering och återställning fungerar på tillfredställande sätt bör företaget minst en gång årligen testa att återställa systemet från säkerhetskopian till en ny maskin, och på så sätt kunna upptäcka eventuella problem.(Mitrovic´, 2003, s. 111-112).

Det är inte bara filer som det behövs ta backuper på, utan även databaser och dess transaktionsloggar. Hur ofta backuper på databaser bör tas beror till viss del på hur länge databasen måste låsas eller på annat sätt ligga nere för att backupen skall kunna genomföras. För databaser med hör dataintensitet blir det således en avvägning mellan att på ett säkert sätt förvara den stora mängden data som ständigt förändras i databasen, och att göra databasen effektiv och användarvänlig i form av snabb svarstid.

För att säkerställa att backupen är till någon nytta bör den placeras på en plats vilken är fysiskt avskiljd från originaldata. Inte sällan är det önskvärt att inneha två separata, speglade backuper, på olika platser vilka båda är avskiljda från originalen. På så sätt är sannolikheten mindre att företaget förlorar värdefull data, ifall någon större katastrof skulle komma att drabba företaget.

5.1.2 Logiskt Intrång

Det finns ett närmast oändligt antal olika attacker och skadliga koder vilka kan komma att skapa problem för ett företag. I detta avsnitt nämns några av de vanligaste attackerna, samt möjlig hantering av dessa.

Inte sällan används portscanning som ett första sätt att identifiera en åtkomstväg in i ett IT-system. Portarna scannas då för att upptäcka eventuella öppna sådana, vilka kan möjliggöra access för en attack. Om lösenord krävs är det ofta möjligt att få tag på ett sådant genom att kontakta systemadministratör eller att använda programvara för att knäcka lösenordet, vilken går att finna på nätet. Sådan programvara kan användas om lösenordet är dåligt skyddat, exempelvis om det inte är krypterat eller om lösenordsfilen lagras på icke tillfredsställande sätt (Heickerö & Larsson, 2008, s. 74). Ett sätt att hantera problematiken med port scanning är att konfigurera brandväggen så att denna är observant, exempelvis gällande antalet paket som mottas under viss tidsrymt Brandväggen bör också ha regler vilka avbryter eventuella attacker, exempelvis genom att vidta åtgärder vid fler än tio portscans inom en minut (Beaver, 2010, s. 127-128).

En utav de vanligaste attackerna som företag utsätts för är så kallade överbelastningsattacker (DoS/DDoS). Ett exempel på användningsområde för en DoS-attack är att överbelasta en webbsida till dess att den kraschar, vilket därmed gör den oåtkomlig för användare. På så sätt begränsas företagets förmåga att sprida information. Attacken kan fungera så att en stor mängd datorer smittas av maskar, vilka vid ett och samma tillfälle börjar anropa webbsidan. Om den stora mängden simultana anrop är fler än vad webbsidan klarar av får attacken en krasch som resultat. (Heickerö & Larsson, 2008, s. 76-77). Det positiva med DoS

attacker är att de vanligtvis är relativt lätta att upptäcka och rätta till, förutsatt att en uppdatering för mjukvaran finns tillgänglig. Finns en lämplig uppdatering inte tillgänglig kan DoS attacker få förödande konsekvenser, så som förstörd eller stulen värdefull data. (Crume, 2000, s. 137) Oskyddade Transmission Control Protocol (TCP) ändpunkter är ett exempel på område vilket är känsligt för DoS-attacker. En DoS attack mot en sådan ändpunkt innebär att antalet Transmission Control Block (TCB) överskrids, vilket skadar serverns tillförlitlighet. DoS-attacker mot TCP-ändpunkter kan förhindras genom att använda Stream Control Transmission Protocol (SCTP) istället för TCP. SCTP är precis som TCP ett tillförlitligt transportprotokoll, men en utav skillnaderna mellan de båda är att en SCTP server förblir ”stateless” under inledningen av handskakningen. Detta då en så kallad state cookie är obligatorisk i SCTP, medans den är frivillig i TCP. En sådan state cookie förhindrar de DoS-attacker som TCP kan utsättas för (Nordhoff, 2006, s. 17-18)

Structured Query Language (SQL)-injektioner är en form av attack som utnyttjar dåligt skriven kod. Den möjliggör åtkomst till databaser och system utan tillgång till korrekt lösenord. Om DDoS inkluderas i en SQL-injektionsattack är intrånget mycket svårt att upptäcka och kan dessutom få förödande konsekvenser. Vid en sådan attack mot en databas finns risk att all data manipulerats. Den ursprungliga informationen kan vidare användas för framtida attacker. Speciellt känslig är situationen om hackern fått tillgång till värdefulla användarnamn och lösenord, vilket möjliggör för denne att maskera sig vid eventuella framtida intrång. (Carr, 2009, s. 141-142) Fördelen med SQL-injektioner är att de är förhållandevis lätta att skydda sig mot, det räcker med att skriva koden ”rätt”.

En brandvägg är inte lösningen på ett företags alla problem, däremot kan en brandvägg vara en bra start på vägen mot en säkrare IT-miljö. Exempel på vad en brandvägg kan förväntas hantera är (Crume, 2000, s. 77-78):

- **Isolera företagets nätverk från andra nätverk**
  Vilken typ av trafik som ska släppas in till företagets nätverk kan hanteras av brandväggen, företaget sätter då själva parametrarna.
- **Isolera delar av det egna intranätet**
  Med en brandvägg kan även det interna nätet delas upp i mindre delar, vilket kan vara användbart om endast vissa grupper ska ha tillgång till viss information
- **Erbjuda en enstaka punkt för passering in i och ut ur nätverket**
  Detta gör det lättare att kontrollera säkerheten

Det bör dock också klargöras att det finns en hel del komplikationer att ta hänsyn till när det gäller brandväggar. Sådana kan exempelvis vara (Crume, 2000, s. 79-80):

- **De bör ej ligga på samma plattform som andra applikationer**
  Om något program havererar kan det skapa hål i brandväggen, vilket kan vara skadligt för företaget. Det gäller därmed att inte vara dumsnål, trots att det kan vara frestande att lägga ihop brandväggen med annat för att spara pengar.
- **Brandväggen får inte vara tillåtande per default**
  Defaultinställningarna bör vara att ingenting är tillåtet, vilket innebär att företaget måste tillåta all trafik explicit. Därmed minskar risken för att någonting glöms bort eller slinker igenom.

- **Information bör inte lämnas om nätverksdetaljer**
  För att dölja detaljer om nätverket, så som nätverksadresser, kan exempelvis applikationsproxies och SOCKS användas. Ju mindre information en hacker får, desto svårare blir dennes jobb.

- **En brandvägg är ej till för att stoppa virus**
  Brandvägg och antivirusskydd är helt olika saker, det är därför viktigt att förstå att den ena inte kan ersätta den andra. Istället behöver ett företag använda sig av båda delar för att nå en säker IT-miljö.

Med hjälp av Intrångsdetekterings- och kontrollsystem (IDS) kan intrång upptäckas och, om så önskas, åtgärdas. IDS kan övervaka samtal, loggar, trafikmönster osv. Om ett intrång detekteras informeras systemägaren, vilken utför åtgärder. Det går även att installera systemet så att åtgärder utförs automatiskt, då är det tal om intrångsprevention. Ett sätt att varna företaget om någon försöker utföra en attack är att använda falska noder, ”honeypots”. Dessa kan användas som lockbete och övervakas av IDS, för att sedan fånga in eventuella hackare. (Heickerö & Larsson, 2008, s. 109-110).

Ett effektivt sätt att försvåra för en attackerare är att hålla all lagrad data krypterad. På så sätt försvåras hackerns arbete, och i bästa fall gör det till och med bytet tillräckligt oattraktivt för att motverka attacker.

5.1.3 Kryptering

Oavsett om säkerhet diskuteras ur ett logiskt eller fysiskt perspektiv, gällande lagrad data eller data under överföring, så finns det ett skydd som är gemensamt för alla dessa: kryptering. Att kryptera data försvårar för inkräktare, oavsett om denne attackerar företaget genom att stjäla hårdvara, hacka sig in i datasystem, eller tjuvlyssna på paket under överföring.

Kryptering av lagrad data görs vanligen genom att kryptera känsliga filer, eller så krypteras hela hårddisken. Det sistnämnda underlättar för användaren, i och med att denne på så sätt inte behöver fundera kring vilka filer som behöver krypteras. Kryptering av hela disken kan göras i antingen hårvaran eller mjukvaran. Det finns dock en nackdel med kryptering av hela hårddisken. Denna lösning kräver mer administration, exempelvis om hårddisken kraschar eller krypteringsnyckeln förloras. (Eriksson & Fogel, 2008, s. 3) Företaget bör således göra en avvägning för varje dator, där säkerhet vägs mot enkelhet. Som nämnts tidigare ska det aldrig kosta mer att skydda data, än vad de data som ämnas skyddas är värd.

Det finns idag något som kallas Encrypting File System (EFS), vilket är en krypteringsteknik skapad av Microsoft. Denna teknik är skapad för att snabbt kryptera filer på en hårddisk samt för att underlätta för användaren då filer hanteras, exempelvis vid förflyttning. Med EFS skapas ett certifikat och en krypteringsnyckel vid första krypteringen. Därefter hålls filen krypterad, även då filen flyttas till ny mapp eller hårddisk. Då EFS är inbyggt i operativsystemet behöver filen inte dekrypteras innan förflyttningen sker. Vidare är användaren genom EFS skyddad mot förlust av den privata krypteringsnyckeln, i och med den specialdesignade EFS-återställningsagenten.(Elcomsoft, 2007, s.3)

Det finns idag en uppsjö av krypteringsalgoritmer, de flesta med både kända svagheter och styrkor. Vilken av alla dessa algoritmer som ska väljas i vilket sammanhang är närmast en vetenskap i sig, varför en sådan diskussion inte kommer att föras i denna uppsats. Istället

uppmuntras företag mer generellt att faktiskt använda sig av kryptering. Det är sedan upp till varje enskilt företag att studera tillgängliga algoritmer utifrån företagets aktuella behov, samt att när så behövs ta hjälp utav en säkerhetskonsult för att välja den form av kryptering som passar företaget bäst.

5.1.4 Loggbok

En del i att minska risken för insiderbrott är kravet på att företag ska skriva loggbok över vem som fått ta del av känslig information och när. Loggbok förs dels vid löpande hantering av insiderinformation, som exempelvis vid offentliggörande av årsredovisning och liknande, dels vid mer unik hantering av eventuellt kurspåverkande situation, så som vid budgivningar (OMX, 2008). Då personer får tillgång till känslig information skall detta föras i loggboken, oavsett om personen är anställd på företaget eller inte (OMX, 2008). Förteckningen ska beskriva vem som delgetts information, anledningen till detta och datum då delgivning skett (Lag 2000:1087). Även om det inte är lagstadgat så rekommenderas också att införa klockslag då informationen överlämnats. Loggboken ska uppdateras löpande och senast samma dag som händelsen inträffats. En ansvarig, vanligtvis VD, för då in informationen i loggboken och informerar även personen som delgivits information om att denne nu återfinns i journalen. För återkommande händelser måste denna procedur inte göras varje gång. Istället kan rutiner införas, vilka beskriver vilka som får ta del av information och när i tiden. Då processen påbörjas informeras de involverade personerna om detta, men loggboken behöver inte föras lika detaljerat.

Varje kurspåverkande händelse ska ha sin egen loggbok, alltså kan flera loggböcker föras parallellt på ett företag. Hur dessa loggböcker förs i praktiken och i vilket format de lagras är upp till företaget att avgöra. Den ansvarige får själv, utifrån eget omdöme, besluta kring lämplig hantering, men måste samtidigt tillgodose säkerhetsbehovet kring boken. Rimligtvis bör denna loggbok dock omfattas av samma regler och föreskrifter som för företagets redovisningshandlingar, vad gäller säkerhet, förvaring och åtkomst(OMX, 2008). Efter att den sista uppdateringen gjorts i loggboken skall denna sparas i fem år(Lag 2000:1087). Syftet med loggboken är dels att underlätta kontroller av företagets informationsgivning och eventuella insiderbrott, dels att göra involverade personer medvetna om att de delgivits icke offentliggjord information, vilken inte får vidarelämnas till tredje part. Om information trots detta skulle läcka ut till obehörig part är det viktigt för företaget att ha rutiner för att snabbt offentliggöra den aktuella informationen, inte minst om de till följd av orättvis handel utsatts för handelsstopp(OMX, 2008).

Bland de rekommendationer som OMX sammanställt för säker loggbokshantering nämns bland annat att, i den mån det går, undvika att skriva ut och kopiera företagskänslig information (OMX, 2008). Företaget bör således eftersträva att lagra all känslig information i digital form. Dock kräver det att den digitala informationen skyddas effektivt. Rekommendationerna nämner vidare att handlingar vilka skickas med e-post bör krypteras eller på annat sätt göras oläsbara för obehörig part. Det ska också finnas rutiner för hur känslig information lagras på företagets datorer, även detta för att hindra åtkomst av obehörig person (OMX, 2008).

Varje företag bör införa en policy kring vem som tillåts editera i loggboken samt vem eller vilka som har läsaccess till densamma. Vidare bör loggboken, som ovan nämns, lagras på ett säkert sätt, precis som övrig känslig information. Förslagsvis är loggboken lagrad i ett format vilket inte är läsbart för obehöriga, alltså bör den krypteras. Mer om kryptering finns att läsa i avsnitt 5.1.3.

Ett sätt att säkerställa att endast behöriga personer ges möjlighet att editera loggboken är att använda digitala signaturer. En digital signatur är en kryptografisk teknik vilken kan beskrivas som ett sätt att *”ingå ett avtal”* med innehållet i ett dokument. Det måste således vara möjligt att säkerställa att en ett dokument signerats av en viss person, och inte av någon annan.(Kurose & Ross, 2010, s. 735) Om digitala signaturer kombineras med datering av signaturen kan företaget i efterhand, vid behov, visa alla personer som läst och editerat loggboken, samt när denna tillgång till loggboken ägt rum. Samma teknik, men med viss utvidgning kan även användas för att säkerställa att personer som ska få tillgång till viss information endast får det inom givet tidsintervall. I och med att den digitala signaturen är personlig kan behörighet att exempelvis läsa ett dokument läggas upp så att personer måste läsa dokumentet i viss ordning, efter visst datum, etc. I och med signeringen går det också att i efterhand visa vilka personer som faktiskt fått tillgång till informationen och när detta delgivande skett.

5.1.5 Fysiskt Intrång

Att företagets IT-system är skyddat mot logiska missöden är inte tillräckligt, då inte ens det bästa antivirusprogrammet eller den mest effektiva brandväggen hjälper vid exempelvis en vattenläcka, ett inbrott eller en brand. Företaget måste således även säkerställa att ett fysiskt skydd finns. Ett första steg i den fysiska säkerheten är att införa ett strikt in- och utpasseringssystem på företaget, där obehöriga inte tillåts ströva runt fritt i lokalerna. Lämpligen bör besökare skrivas in vid ankomst och endast vistas i företagets lokaler i sällskap av en anställd. Givetvis bör kontorslokalerna också vara larmade när de är tomma, i hopp om att avskräcka inbrottstjuvar. (Mitrovic´, 2003, s. 103-104). Skärmar bör vara vända bort från fönster och gemensamma utrymmen och faxmaskiner och printers placerade så att besökare inte ges naturlig access. (Mitrovic´, 2003, s. 105). För att försvåra tillgång till information från en annans dator bör alla datorer låsas efter viss inaktivitet. Vidare bör verktyg finnas för att på ett enkelt sätt låsa fast datorer, alternativt rutiner för att lämna dessa i säkerhetsskåp vid dagens slut. Datorer som inte längre är funktionsdugliga och därför går till försäljning eller återvinning utgör också en risk. Företaget måste se till att all data på dessa datorer är tillintetgjord innan datorernas lämnas bort. Att endast radera alla känsliga filer på datorn, för att sedan tömma papperskorgen, har inte på något sätt som resultat att filerna är permanent försvunna. Istället har platsen endast lämnat tillgänglig för ny data, varför den ursprungliga går att återställa till dess att den blivit överskriven. För att fullständigt radera data kan datorn antingen lämnas in till någon som gör detta professionellt, eller göras av företaget självt, med hjälp av något av de många program som finns tillgängliga. Exempel på sådana är Darick’s Boot and Nuke (DBAN), CyberCide och KillDisk. Alla dessa är för Windows, men program med samma funktion finns även för andra operativsystem.(web.mit.edu, 2011)

Sådant som servrar, nätnav och liknande bör lämpligen förvaras avskiljt från resten av kontoret, i en del som inte är speciellt trafikerad, eller i en separat byggnad. Till denna datahall bör endast ett fåtal, behöriga personer ha access. Datahallen bör också inredas på ett sådant sätt att risk för dammansamling, brand, översvämningar och liknande minimeras. (Mitrovic´, 2003, s. 105). Det finns ett antal förutsättningar att ta hänsyn till vad gäller miljön i en datahall. Först och främst är det viktigt att ha kontroll på värmeutvecklingen. Om hårdvaran blir för varm finns det risk för att elektroniska komponenter slutar att fungera. Det är givetvis också viktigt att skydda hårdvaran från vatten. Vidare kan för låg luftfuktighet resultera i uppbyggnad av statisk elektricitet. För hög luftfuktighet kan istället leda till kondens vilken kan orsaka rost och

korroderande metallytor. Mat, dryck, smuts och damm ska alla undvikas i datorhallar. Slutligen är det viktigt att eltillförseln är jämn och pålitlig, (Shim, Qureshi & Siegel, 2000, s. 14)

Företag som är mycket beroende av tillgång till dess data bör överväga en speglad datorhall på en plats helt separerad från den ordinarie. Detta är en mycket kostsam lösning, i och med att företaget måste betala för dubbla lokaler, hårdvara, osv. Dock är det ett effektivt skydd mot exempelvis brand, som gör det möjligt att närmast eliminera risken för ett avbrott. En billigare lösning är att dubbla nyckelkomponenterna i systemen, tillsammans med ett serviceavtal, vilket möjliggör för en tekniker att snabbt ge sig ut och byta komponenter vid eventuellt haveri. Det är upp till varje företag att värdera risken mot kostnaden, och fatta beslut därefter. (Mitrovic´, 2003, s. 106). En ytterligare försäkring som kan vara intressant att nämna är Uninterruptible Power Supply (UPS). UPS fungerar som ett batteri vid ett totalt strömavbrott och försörjer systemen med ström samtidigt som det avslutar processer på ett korrekt sätt. På så viss minskar risken för att data går förlorad. (Mitrovic´, 2003, s. 107).

Utöver den risk som finns för stulen eller skadad data på servrar finns ett annat problem: laptops. Laptops medför många underlättar vardagen för många företag, i och med att de kan medtagas till möten, både externa och internt, användas för åtkomst av Virtual Private Network (VPN) hemifrån och från utlandet, osv. Detta får som resultat att laptops ofta transportera utanför företagets väggar, och skyddas således inte utav de eventuella säkerhetsansträngningar som finns där. Att laptops därmed löper större risk för att bli borttappade eller stulna än stationära datorer medför att data lagrad på laptops är extra utsatt. Lämpligen bör laptops som förflyttas utanför företaget vara utrustade med program vilka försvårar tillgång till information på datorn för en obehörig. Den information som finns på datorn bör det även ha tagits backup på, för att den inte ska gå förlorad ifall datorn blir stulen. För att till det yttersta säkerställa att ingen känslig information hamnar i fel händer ska speciella, rena laptops användas vid resor. Alternativt kan den egna datorn användas, men tömmas på all känslig information innan avresa.(fb.gov, 2011) Affärshemligheter så som recept, information kring kundstocken etc. bör aldrig förvaras på laptops, USB-minnen och andra enheter som lätt hamnar i orätta händer. För att säkerställa att så inte sker inför företaget lämpligen en policy gällande vilken information som aldrig får finnas på vilka enheter. Denna policy måste sedan kommuniceras till hela personalen, för att undvika missöden.

5.2 Data under överföring

Ett företag kan också utsättas för trafikavlyssning, där någon ”sniffar” Internettrafiken. Detta kan göras bland annat för att spionera på användare och samla in information och för att dekryptera känslig sådan. Dock kan företag även använda sig av denna teknik för att upptäcka eventuella attacker eller intrångsförsök. (Heickerö & Larsson, 2008, s. 76-77).

5.2.1 Kommunikation mellan kontor/affärspartners

Ett sätt att skapa ett säkert nätverk, vilket är helt oåtkomligt för obehöriga är att bygga ett så kallat privat närverk. Privata nätverk är fysiskt helt avskiljda från Internet, med egna routrar, länkar och egen Domain Name System (DNS)-infrastruktur. Även om privata nätverk är säkra är de inte alltid intressanta för företag då de oftast ör mycket kostsamma.(Kurose & Ross, 2010, s. 760) Ett mer ekonomiskt sätt att koppla huvudkontoret till andra kontor eller affärspartners, lokaliserade i olika städer eller länder, är genom en VPN-tunnel. VPN är ett nätverk vilket användaren upplever som ett separat, fysiskt nätverk, trots att nätverket inte är privat i fysisk mening. Istället är det en del av en delad infrastruktur, men med säkerhet motsvarande den för

ett dedikerat nätverk. En VPN-tunnel är således ett sätt att ”tunnla” trafik från avsändare till mottagare på ett säkert och privat sätt. (Crume, 2000, s. 243-244) Trafiken krypteras då innan den skickas över det publika Internet. En VPN-tunnel kan skapas med hjälp av en brandvägg. Funktionaliteten finns dock inbyggd i ett flertal operativsystem, vilket möjliggör tunnling även utan tillgång till brandvägg. Säkerheten för en VPN-tunnel kan höjas avsevärt genom användandet av protokollet IP Security (IPSec) (Mitrovic´, 2003, s. 179). IPSec erbjuder säkerhet på nätverkslagret och säkrar IP-datagram mellan exempelvis hosts och routers (Kurose & Ross, 2010, s. 760).

5.2.2 E-mejl

Många företag använder idag e-mejl som huvudsaklig skriftlig kommunikation. Kontrakt, mötesprotokoll och andra företagskänsliga data skickas per e-post, både internt och externt. För att företaget ska kunna använda detta kommunikationsmedel utan att äventyra verksamhetens säkerhet måste e-mejl med känsligt innehåll skickas på sådant sätt att obehöriga ej kan ta del av innehållet eller på annat sätt orsaka skada för företaget. Det finns ett antal önskade egenskaper för säker e-postkommunikation (Kurose & Ross, 2010, s. 748):

- *Konfidentiell kommunikation:* Endast avsändare och avsedd mottagare ska kunna ta del av innehållet i det som skickas. Då det finns risk för att någon tjuvlyssnar på kommunikationen kräver detta någon form av kryptering
- *Ändpunktverifiering:* Både avsändare och mottagare ska kunna att den andra partens identitet är korrekt
- *Meddelandeintegritet:* Det ska vara möjligt att säkerställa att det meddelande som skickades är detsamma som det som mottagits

Alla punkterna ovan är viktiga vid e-mejlkommunikation. För att åstadkomma kommunikation vilken uppfyller alla punkterna ovan kan ett två metoder kombineras: Kryptering med en symmetrisk nyckel och digitalt signerade hashfunktioner. Ett nytt meddelande skapas utifrån det som ska skickas, vilket består av ursprungsmeddelandet tillsammans med en digitalt signerad hashfunktion av detta. Detta nya meddelande krypteras med avsändarens privata nyckel och mottagarens publika nyckel. På samma sätt dekrypteras meddelandet av mottagaren med dennes privata nyckel, samt avsändarens publika. Detta sätt att skydda meddelanden är i dem alldra flesta fall tillfredsställande. Dock bygger säkerheten på att avsändare och mottagare bytt nycklar med varandra på ett säkert sätt. Risken finns att någon obehörig utger sig för att vara någon av parterna och därmed kan lämna ut en felaktig nyckel och på så sätt tillgodogöra sig information olovligen.(Kurose & Ross, 2010, s. 750) Dock kan det här vara värt att påminna om att den traditionella brevväxlingen inte på något sätt är ett fullkomligt säkert alternativ till e-posten. En person med avsikt att lägga beslag på dokument som skickas med vanlig post har ett förmodligen mycket enklare jobb en den som måste dekryptera e-postmeddelanden.

Utöver uppenbara fördelar så som möjlighet till snabb respons och kostnadsbesparingar, finns ytterligare fördelar för företag med att använda sig av e-mejl. En utav dessa är att det är lätt att härleda kommunikation och visa upp dokumentation i efterhand, om kommunikation skett via e-post. Företaget kan således visa i vilken ordning viss konversation skett och när i tiden. Det är på så sätt också lätt att påvisa vilka personer som delgivits viss information. Sådana referenser kan visa sig värdefulla om meningsskiljaktigheter eller orätt skulle uppstå.

5.2.3 VoIP telefoni

En Internetapplikation som nått hög popularitet senaste åren är VoIP. Tekniken erbjuder ett billigt alternativ till användande av traditionella telefonlinor, Public Switched Telephone Network (PSTN). För företag med behov av samtal mellan olika länder kan detta innebära en enorm kostnadsbesparing. Istället för att samtalet processas över kommersiella telefonlinjer kan samtal istället föras över Internet, eller privata nätverkslinor. (Kuhn, Walsh & Fries, 2005, s. 21). En vidare fördel med tekniken är att det går att ringa både till andra VoIP användare och till analoga telefoner. (Kuhn, Walsh & Fries, 2005, s. 18). Men det finns också risker med VoIP. Företaget bör ej införa IP-telefoni förrän risker och fördelar vägts mot varandra (Halpern, 2003, s. 2).

Det ständigt ökade intresset för denna tjänst gör den sannolikt till nästa mål för attackerare. Att attacker specifika för VoIP växer fram är ingen orealistisk förväntan (McGann & Sicker, 2005, s. 1). En vanligt förekommande missuppfattning är att VoIP är säkert så länge nätverket är säkert. Tyvärr räcker det inte med ett säkert nätverk, då VoIP adderar ett antal komplikationer till den existerande nätverkstekniken (Kuhn, Walsh & Fries, 2005, s. 8). Det finns en stor mängd svagheter med VoIP, inte bara avseende själva applikationen, utan också kopplat till operativsystemet samt applikationer och protokoll vilka VoIP förlitar sig på. (McGann & Sicker, 2005, s. 1). Säkerhetsrisker kopplade till IP-telefoni ligger mycket närmare de som ofta diskuteras gällande datorer på IP-nätverk än de risker som finns i vid användning av traditionell telefoni. En stor skillnad jämfört med PSTN är att de traditionella linorna måste attackeras fysiskt för att komproteras, alternativt måste företagets 'Private Branch Exchange' (PBX) attackeras. Detta har inneburit att endast ett fåtal företag bemödat sig med att kryptera dess telefonsamtal. Vad gäller VoIP är situationen en helt annan. Datapaketen skickas utan kryptering i klartext och görs på så sätt tillgängliga för vem som helst med grundläggande kunskaper i hur attacker utförs.(Kuhn, Walsh & Fries, 2005, s. 23) Av skäl relaterade till QoS, skalbarhet, hanterbarhet och säkerhet bör IP-telefonin segmenteras från nätverket vilket hanterar IP-data. På så sätt kan samma access, kärna och distributionslager användas, utan behov för två IP-infrastrukturer.(Halpern, 2003, s. 4) Det finns idag en mängd krypteringsprodukter för VoIP, vilka kan hjälpa företag att skydda dess IP-telefonisamtal.

En fullständig förteckning över svagheter återfinns i Appendix B. För att identifiera aktuella svagheter kan företaget ta hjälp av program vilka scannar systemet på jakt efter säkerhetsluckor (motsvarande är inte sällan använda av attackerare), så som exempelvis SiVuS, PROTOS c07-SIP Test Suite och SIP Forum Test Framework (SFTF) (McGann & Sicker, 2005, s. 3-5). Om sådant program används är det dock viktigt att ha i åtanke att dessa inte är fullständiga eller felfria. Ett resultat som visar på avsaknad av brister behöver inte nödvändigtvis tala sanning, vissa svagheter går inte att finna med existerande program. Programmen bör därför användas som en fingervisning och inte som facit.

Utöver säkerhetsrisker finns också möjliga problem vad gäller kvalitet på samtalen. Om alla anställda på ett företag ersätter den traditionella telefonin med VoIP blir belastningen på det interna nätverket hög. Detta riskerar resultera i förstoppning, vilket snabbt sänker samtalskvaliteten (Kuhn, Walsh & Fries, 2005, s. 8). I och med de ständigt ökande bredbandshastigheterna är detta dock ett problem som sannolikt är snart övergående.

En uppsjö av rapporter vilka berör VoIP och lösningar på existerande säkerhetsbrister går att finna på nätet. Om intresse finns för att skapa en säker miljö för IP-telefoni finns det således mycket hjälp att tillgå.

I och med att VoIP i mångt och mycket fungerar som annan IP-trafik finns också möjlighet att ta del av de fördelar som finns kring sådan kommunikation. Om eventuella säkerhetshål täpps igen kan IP-telefoni användas som ett säkrare alternativ till traditionella telefonlinor, där de parter som deltar i samtalet kan nyttja samma säkerhet som vid exempelvis e-post. På så sätt kan kommunikation ske konfidentiellt, de olika parterna verifieras och integritet säkerställas. Om alla samtal dessutom spelas in kan företag i efterhand använda dessa som referens, ifall det skulle föreligga oklarhet kring exempelvis delgivande av viss information.

5.2.4 USB-minnen och andra portabla enheter

Som nämnts tidigare är det inte att rekommendera att lagra data på enheter vilka är lätta att tappa bort eller få stulna. Innan företaget lagrar data på sådana enheter, vilka USB-minnen och CD/DVD skivor är exempel på, bör ett övervägande göras. Endast information som nödvändigtvis måste finnas på sådana enheter ska få placeras där.

Även om USB-minnen är relativt små kan dataintrång till följd av undermåligt hanterade USB-minnen få enorma konsekvenser. Många företag är medvetna om de risker som användande av USB-minnen är förenade med, men få arbetar aktivt för att hantera dessa risker.(Ponemon Institute, 2011, s. 14) Exempelvis är det vanligt att anställda överför information till USB-enheter utan att i förväg få tillstånd att göra så. Ofta låter anställda dessutom bli att rapportera stulna eller förlorade USB-minnen.(Ponemon Institute, 2011, s. 4) Ett sätt att förbättra säkerheten kring USB-minnen är att införa policys, vilka uttrycker hur USB-enheter ska användas på ett säkert sätt, samt vilken behandling av dessa enheter som är förbjuden. För att sådana policys ska ha effekt är det viktigt att företaget arbetar aktivt med den, exempelvis genom träningsprogram. (Ponemon Institute, 2011, s. 5) Utöver föreskrifter kring hur portabla minnen ska användas finns det mycket företaget kan göra. Bland annat bör all data på USB-minnen krypteras, informationen på dessa enheter bör granskas och godkännas och de skyddas lämpligen med lösenord (Winencrypt, 2009, s. 2).

5.2.5 Smartphones

Användandet av smartphones är idag vida utbrett och används av alltifrån regeringar till företag och privatpersoner. Det är framförallt smartphonens mångsidighet som gjort den känd. Den kan nyttjas till GPS, e-post, för att läsa streckkoder, surf och för att ringa med, för att nämna några användningsområden (Hogben & Dekker, ENISA, 2010, s. 10). Mobila enheter är, tillföljd av deras natur, mer utsatta för risker så som stöld och borttappning än större system med fixa platser. Visserligen blir mobiltelefoner idag oftare stulna för att tjuven vill komma åt den fysiska produkten, men det finns ändå risk för att det är den data som finns lagrad på mobiltelefonen som är det attraktiva.(Botha, Furnell & Clarke, 2008, s. 131) Vidare så finns en påtaglig risk för att mobiltelefonen används både för privata ändamål, som till socialt nätverkande och att medtagas på långväga semesterresor, och i arbetssammanhang, exempelvis för att hantera känslig information. På så sätt ökar riskerna med smartphones ytterligare, speciellt då konsumentbeteende generellt sett medför högre sannolikhet att drabbas av dataintrång (Hogben & Dekker, ENISA, 2010, s. 12 & 15).

Threat description	The smartphone is stolen or lost and its memory or removable media are unprotected, allowing an attacker access to the data stored on it.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	High	Medium	Medium
Employee (E)	Medium	High	High
High official (H)	Medium	Very high	High
Vulnerabilities	[6.7 Lack of user awareness][6.4 Encryption weaknesses]		
Assets	All		

Figur 3, Sannolikhet, påverkan och risk för olika smartphoneanvändare vid stöld/borttappad telefon(Från ENISAs rapport "Smartphones: Information security risks, opportunities and recommendations for users", s. 15, pulicerad i enighet med föreskrifter)

Även om många datoranvändare har för vana att ge säker hantering till laptops och andra portabla enheter, är det långt ifrån självklart att mobiltelefonen får samma behandling. Inte ens om ambitionen finns där behöver det bli verklighet, då förutsättningar i form av funktionalitet ofta saknas.(Botha, Furnell & Clarke, 2008, s. 131) Om data presenteras på samma sätt i mobiltelefonen som på en dator, men utan samma möjlighet till säkerhet, uppstår det ett säkerhetsglapp. Dessutom erbjuder smartphones möjlighet till nedladdning av applikationer och mottagande av meddelanden, vilka alla kan vara förklädda phishingattacker. Genom applikationer eller meddelanden (exempelvis SMS eller e-post) vilka framstår som genuina, kan telefonen bli föremål för attacker vilka samlar in exempelvis lösenord eller. (Hogben & Dekker, ENISA, 2010, s. 20). Andra attacker som smartphones kan utsättas för är spyware, network spoofing och övervakningsattacker, för att nämna några. Det är också viktigt att företaget till fullo förstör den data som finns på smartphones, innan de tas ur bruk eller säljs vidare. Risken finns annars för identitetsstöld eller att information hamnar i fel händer.(Hogben & Dekker, ENISA, 2010, s. 19)

Det mest effektiva sättet att förhindra de risker som nämns ovan är att helt förbjuda smartphones på arbetsplatsen. Detta är dock sällan önskvärt, då smartphones erbjuder företagen många möjligheter. De anställda är uppkopplade dygnet runt och har ständigt möjlighet att hålla sig uppdaterade och besvara e-post. I och med den ständigt växande mängden applikationer till dessa enheter kommer smartphonen sannolikt att få fortsatt ökad betydelse, både i affärslivet och privat. Företag måste således hitta andra sätt att möta hoten. Till en början måste både slutanvändare och IT-ansvariga få upp ögonen för alla de risker som är relaterade till användning av smartphones, för att komma till rätta med dem. Råd och riktlinjer bör sättas upp för slutanvändare och speciella regler gällande smartphones bör finnas med i företagets IT-policy. I den mån det går bör företaget också motverka dataintrång med tekniska medel, i form av exempelvis defaultkonfigurationer och säkerhetsmjukvara (Hogben & Dekker, ENISA, 2010, s. 42). Anställda bör inte förvara eller processa hemligstämplad information på sina

mobiltelefoner, känslig information krypteras och inforation av värde för användaren eller företaget tas backup på regelbundet.(Hogben & Dekker, ENISA, 2010, s. 43) För en mer genomgående diskussion kring risker kring smartphones och möjlig hantering av dessa rekommenderas ENISAs rapport "Smartphones: Information security risks, opportunities and recommendations for users".

5.3 Trådlös kommunikation

Säkerhet i trådlösa nätverk är en minst sagt nödvändig fråga, framförallt då radiovågorna förmår propagera långt utanför företagets väggar. (Kurose & Ross, 2010, s. 768) Ett trådlöst nätverk kan utsättas för de flesta attacker som ett kablat nätverk kan utsättas för, samt några unika attacker/säkerhetsrisker. Exempel på säkerhetshot det finns risk för är felaktigt konfigurerade Åtkomstpunkter (AP), felaktigt associerade klienter, obehöriga AP:s som kopplas till nätverket, DoS-attacker, IP Spoofing och Hijacking (Siemens Enterprise Communications, 2008, s. 5-6). Det finns ingen lösning som passar alla företag, utan var och ett måste själv göra en avvägning mellan den säkerhetsnivå som krävs och dess övergripande kostnader. Vidare måste företaget införa en säkerhetspolicy för trådlösa nätverk. En sådan policy bör bland annat innehålla information kring vem som får använda det trådlösa nätverket och hur, vilken information som får skickas över trådlösa nätverk och hur kryptering nyttjas.(Siemens Enterprise Communications, 2008, s. 8) För att ett trådlöst Local Area Network (WLAN) ska vara effektivt måste det hantera följande kritiska områden: data kan skickas konfidentiellt och med integritet, verifikation och accesskontoll, samt intrångsdetektering och motverkan.(Siemens Enterprise Communications, 2008, s. 2). Dagens WLAN-system, vilka använder WPA/WPA2 med AES kryptering kan erbjuda relativt god säkerhet vilken åtminstone uppnår den för kablade nätverk (Siemens Enterprise Communications, 2008, s. 14). Om WPA används i ett trådlöst nätverk kan säkerheten förbättras uppgradera till WPA2, andra generationens WPA. Säkerhetsförbättringen är stor nog att motivera kostnaden för de flesta företag. För större företag är WPA2(AES) att föredra framför WPA(TKIP), då attacker endast riktar sig mot den sistnämnda. Väljer företaget att använda TKIP-versionen är det viktigt att ha långa nycklar, på minst 20 tecken. Istället för en DHCP kan statiska IP-adresser användas (eller DHCP som tilldelar statiska adresser), för att på så sätt kräva en viss adress för att stationen ska få ansluta sig till nätverket. Om även MAC-filtrering används innebär det ytterligare ett hinder som en eventuell hacker måste ta sig igenom, ju fler desto bättre. (Olsson, 2006, s. 73-75) Tilläggas kan att både WPA och WPA2 finns i två versioner: Enterprise och Personal, där Enterprise har högre verifieringskrav (WiFi Alliances, 2005, s. 6). WEP bör inte användas av företag, då det inte erbjuder tillfredsställande skydd (Siemens Enterprise Communications, 2008, s. 9).

5.4 Tyst period vs. Transparens

Som beskrivits i tidigare avsnitt kring reglering av börsnoterade bolag kräver lagstiftningen att noterade bolag ska arbeta transparent, och på så sätt ge möjlighet för investerare och andra intressenter att få insyn i företaget. Vidare ska rapporter och annan viktig information snabbt kunna offentliggöras. Dock ska samma rapporter och information förbli hemliga för obehöriga personer, fram till vissa tidpunkter, så som exempelvis tills bokslut släpps. Denna avvägning mellan transparens, snabba offentliggöranden och samtidigt hemlighållande av känslig information är inte alltid helt lätt. Mycket av det material som vid givna tillfällen ska offentliggöras måste förberedas i god tid dessförinnan, men utan att för den sakens skull bli känt av allmänheten, eller ännu värre, av några få obehöriga som kan handla utifrån denna insiderinformation. För att kunna behålla viktig information innanför företagets väggar fram till

offentliggörande krävs en tydlig policy kring informationshantering. Det är också här loggboken kommer in i bilden. Det är viktigt att dokumentera vem som får tillgång till viss information och när, informationen måste lagras på en säker plats och endast hanteras av behöriga. När det till slut är dags för offentliggörande måste detta gå fort, för att allmänheten ska ges möjlighet att handla utifrån samma information, samtidigt. I policyn bör således även ingå hur inforationen ska spridas, exempelvis via hemsidan och pressreleaser.

5.5 Rutiner vid eventuellt intrång

Om olyckan trots alla försök att skydda företagets data ändå skulle vara framme är det viktigt att det finns rutiner för att hantera detta. För att minimera skadorna vid eventuellt intrång är det viktigt att ha en hanteringsplan, redan innan ett intrång sker (Online Trust Alliance, 2011, s. 9) Avsikten är på så sätt att snabbt kunna återställa säkerheten, utan att för den sakens skull förstöra eventuella bevis. Rutiner för krishantering av detta slag måste således tas fram. Organisationen bör vara redo att snabbt informera alla berörda parter om eventuellt intrång, inklusive myndigheter. Informationen som lämnas ut måste vara korrekt och eventuell ersättning till utsatta intressenter redan påtänkt.(Online Trust Alliance, 2011, s. 9)

För den oerfarne finns risk att den första instinkten är att återställa hela systemet, för att på så sätt snabbt få upp säkerheten igen och avbryta ett eventuellt intrång. Det behöver dock inte nödvändigtvis vara rätt väg att gå. På så sätt riskerar företaget att förlora tillgången till värdefulla bevis, inte bara på vem som kan ha utfört en attack, utan också gällande vilken information som faktiskt attackeras. För att undvika sådana förhastade felaktigheter är att av yttersta vikt att det finns tydliga riktlinjer. Ett team bör sammansättas redan innan ett intrång sker, för att tydliggöra vem som ska kontaktas om ett intrång upptäcks. Vidare bör det i planen finnas uttryckt vilka myndigheter som ska kontaktas, mallar bör vara framtagna för rapportering av intrång och anställda bör utbildas för att på bästa sätt kunna följa de riktlinjer som satts upp. (Online Trust Alliance, 2011, s. 10)

6 Vem och Vad?

För att företaget ska ha möjlighet att förhindra eventuella dataintrång är det viktigt att skaffa sig en bild över vad hackers kan tänkas vara ute efter, varför de vill åt detta samt hur de avser komma åt önskad data (Crume, 2000, s. 20). Det är också nödvändigt att försöka förstå vilken information som kan vara av värde för en inkräktare, för att på bästa sätt kunna skydda denna.

6.1 Hacker och Motiv

Ett ord som ofta används när det talas om inkräktare och dataintrång är *hacker*. I denna uppsats används ordet hacker som samlingsnamn för alla typer av inkräktare vilka försöker ta sig in den elektroniska vägen. Vissa gör skillnad på hackers och crackers, där den sistnämnde är en person med onda avsikter. Andra pratar istället om ”white hats” och black hats”, även här är den senare nämnda en person som inte har goda avsikter. Alla dessa går alltså här under benämningen ”hacker”, eller ”attackerare”.

En hacker är en person med mycket goda datorkunskaper, vilken med hjälp av dessa kan ta sig förbi avancerade säkerhetssystem. Syftet med en sådan attack kan exempelvis vara att tillgodogöra sig hemlig information, stjäla lösenord eller manipulera hårdvara och/eller mjukvara. (Heickerö & Larsson, 2008, s. 55-56).

Processen för en hacker vilken förbereder ett dataintrång ser vanligtvis ut som följer (Heickerö & Larsson, 2008, s. 77):

1. **Internetbaserade nätverksmöten**

   Avancerade hackers är ofta organiserade i communities, vilka utbyter information och programvara med varandra. Om hackern ingår i ett sådant nätverk är det möjligt att denna tar hjälp av andra hackers. Därefter inleds fasen för IT-Spaning, vilken innefattar punkt 2-4 nedan och går ut på att undersöka och kartlägga motståndarens (företagets) IT-system.

2. **Omfattande kartläggning av målobjekt**

   Vanligtvis genomför en noggrann och tidskrävande analys innan själva intrånget påbörjas. Kapacitet och struktur analyseras. Mönster och stuktur eftersöks, precis som information kring vilken mjukvara som används, plats för databaser, externa samarbetspartners, osv. (Heickerö & Larsson, 2008, s. 77).

   Detta kan exempelvis göras med hjälp av disassembler, vilken presenterar mjukvaran i maskinnära kod. Detta gör det möjligt att studera mjukvaran i detalj och finna eventuella buggar eller säkerhetsbrister. Hårvaran kan analyseras med så kallad ”reversed engineering” om leverantören är känd, vilket riskerar blotta säkerhetsluckor. Ett sätt att identifiera de program och operativsystem som används är med hjälp av så kallad ”finger printning”. Detta är en metod för att analysera de paket som skickas. (Heickerö & Larsson, 2008, s. 72-73).

3. **Exploatering av brister och sårbarheter**

   Spaningen syftar till att presentera en fullgod bild över vilka attacker som är möjliga att genomföra. (Heickerö & Larsson, 2008, s. 72-73). Inte sällan delar hackers med sig av

program specialskrivna för att utnyttja viss brist eller sårbarhet till jämlikar. Detta för att få något i utbyte eller för att göra sig ett namn i hackerkretsar.

4. **Inventering av möjliga angreppsmetoder**

Ett sätt att undersöka möjliga attacker är att skapa en DOS-attack med syfte att överbelasta och i värsta fall krascha systemet. Företagets tillgängliga IT-resurser förväntas då ägna sig åt att lösa problemet, vilket kan ge en fingervisning om vilka resurser företaget har samt organisationens kompetens och rutiner för krissituationer. Då spaningen är utförd kan hackaren gå vidare till den faktiska attackfasen.

För att kunna skydda sig mot dataintrång av olika slag är det viktigt att först av allt måla upp en bild av den potentiella hackern. Vad har denne person för drivkrafter? Vilka kunskaper har hackern? Vad vill han/hon komma åt?

Vanligast är att dataintrånget kommer utifrån och att hackern därmed är en extern person (Verizon Business, 2011, s. 18). Andelen externa hackers har ökat, och med det också standardisering av deras metoder. Det blir allt vanligare att en och samma hacker gör intrång på en mängd platser, genom att återanvända en och samma metod. Anledningen till den stora ökningen av externa hackers är sannolikt att det idag går att nå skalekonomi genom dataintrång.(Verizon Business, 2011, s. 19) Det mest förekommande attackerna är de som skickar data till utomstående site eller enhet, öppnandet av bakdörrar för att på så sätt ge tillgång till acces/kontroll på avstånd och intrång som syftar till att ta reda på någon form av användardata eller lösenord. I de allra flesta fall görs detta med hjälp av hacking eller skadlig kod. (Verizon Business, 2011, s. 27) Oftast är det servrar och användarenheter som attackeras. (Verizon Business, 2011, s. 44)

De siffror som nämns ovan är ett snitt över en mängd företag och branscher. Det är således ingenting som det enskilda företaget bör luta sig mot. Istället är det upp till varje företag att göra en egen analys av de data och den information som företaget äger. I analysen kan det vara av intresse att studera vilken data som kan vara av värde för någon annan, och i så fall för vem? Kan konkurrenter kan vara intresserade? Eller kriminella organisationer? Utifrån svaren på de frågor företaget ställt bör sedan en policy utformas, där den information som är mest känslig och den som är mest trolig att vara av värde för någon annan skyddas högst. Ibland behöver företaget inte gå så långt som till kriminella sammanslutningar eller spionerande konkurrenter för att finna en potentiell inkräktare. Ibland räcker det med en missnöjd anställd, en intern hacker.

6.1.1 Hotet inifrån

En intern hacker, eller insider, är en attackerare som befinner sig inom en organisation. Denne kan antingen vara planterad där av någon utifrån, eller vara en anställd vilken av någon anledning fattat missnöje mot sin arbetsgivare. Konsekvenserna av en vad en insider kan åstadkomma kan bli enorma. (Heickerö & Larsson, 2008, s. 57).

Många företag fokuserar på att skydda intern data mot yttre hot. Det är då lätt att glömma hotet som kommer inifrån: de anställda. Under många låg andelen intrång utförda av en insider legat och pendlat runt omkring 50 % (Richardson, 2008, s. 14). Idag är denna andel nere på närmare 10 %, men det är snarare på grund av att antalet externa hackers ökat än att de interna minskat (Verizon Business, 2011, s. 18). En insider har många fördelar jämfört med en extern

hacker, eftersom insidern förmodligen har kunskap kring vilken data som är relevant och vilken som inte är det, kan företagets säkerhetspolicy (och dess svagheter), har insikt i vilka anställda som helt eller delvis ignorerar säkerhetsföreskrifterna, har fysisk access till känsliga servar och befinner sig innanför brandväggen som skyddar mot omvärlden (Crume, 2000, s. 88). Med detta som grund är det relevant att fundera över om företaget ska införa även interna brandväggar. En intern brandvägg fungerar precis som en extern, men avskiljer istället en del av det interna nätet. På så sätt kan företaget skydda känsliga servrar och liknande, och därmed göra dem tillgängliga endast för behöriga personer (Crume, 2000, s. 88).

Anställda bör också informeras om säkerhetsproblem gällande lösenord. Får användaren själv välja lösenord resulterar det ofta i ett som är lätt att gissa. Om företaget istället tvingar anställda att ha lösenord som är svåra att gissa sig till blir det allt som oftast också svåra att komma ihåg. Detta resulterar i att många skriver ner lösenordet, vilket direkt gör det osäkert (Crume, 2000, s. 107-116). Det gäller därför att finna en balans där lösenordet är relativt lätt att minnas, men svårt att gissa sig till. Riktlinjer för detta bör vara tydligt kommunicerade till personalen. Så fort en anställd slutar på företaget bör dennes lösenord och åtkomsträttigheter tas bort. Om företaget tillåter att anställda som slutar får köpa loss mobiltelefon och/eller laptops är det dessutom viktigt att till fullo ta bort den information som finns lagrad på dessa enheter.

6.2 Vad måste skyddas?

Utifrån svaren på dessa frågor måste företaget fundera kring vad det är som faktiskt borde skyddas. En analys utifrån både en hackares och en försvarares ögon bör således göras, för att på så sätt täcka in så mycket som möjligt av tänkbara säkerhetsbrister och lösa dessa.

Då viss information är ytterst känslig och kan orsaka enorm skada om den läcker ut, medan annan är helt ofarlig, även i fel händer, är det viktigt att klassificera informationen (Mitrovic´, 2003, s. 41). Ett sätt att göra detta är att följa den fyrgradiga skala som används inom den publika sektorn, där det lägsta steget är ”publik information”, vilken anses helt ofarlig om den läcker ut, följt av Känslig information, vilken kan ställa till med begränsad skada, Privat Information, vilket kan vara skadligt för företaget eller anställda och slutligen Konfidentiell Information, vilken alvarligt kan skada företaget (Mitrovic´, 2003, s. 42). Utifrån denna klassificering är det sedan lättare att tilldela informationen lämplig säkerhetsklass.

7 Lagring av data

Att fokusera på säkerhet är idag inte tillräckligt för de flesta företag. Många har också ett behov av att säkra möjlighet till en smidig, eventuell, framtida expansion. Med detta som grund görs nedan en kortare jämförelse mellan fysisk och logisk IT-drift. Därefter tas problematiken kring lagreglerad lagring av data upp.

7.1 Cloud Computing (drift i molnet) *versus* Fysisk hosting

Det finns mycket att diskutera och analysera vad gäller infrastruktur och lagring av data. Bland annat så får fördelarna med att Cloud Computing allt större uppmärksamhet. Cloud Computing innebär att all data och mjukvara hostas på en server eller serverpark, för att vid behov skickas över Internet, utan något större behov utav hårdvara (Delgado, 2010).

Outsourcing av IT är under intensiv diskussion. Bland fördelarna med att lägga ut IT-systemet på entreprenad finns att företaget kan ägna sig åt sin kärnkompetens och låta någon som är IT-kunnig handha IT-hanteringen. Om detta sköts korrekt kan det också leda till effektivisering av IT-systemet, samtidigt som det hanteras mer professionellt. Detta bygger dock på att företaget som IT-systemet lagts ut på bedriver sin verksamhet på ett säkert sätt och har tillfredsställande kontroll av sina anställda, med tanke på insiderproblematiken. (Heickerö & Larsson, 2008, s. 108). En del av kritiken mot Cloud Computing gäller nämligen att det är en tredje part som håller data, vilket medför risk för bristande kontroll från företagets sida samt sämre transparens. (Chow, Golle, Jakobsson, Shi & Staddon, 2009, s. 2)

För många företag väger potentialen dock tyngre än riskerna. Möjligheten för företag att allokera bandbredd, minne, osv. dynamiskt, *On-Demand* är en utav vinsterna, att små företag kan slippa betala dyra uppstartskostnader för att köpa hårdvara är en annan. Ur säkerhetsperspektiv kan också nämnas möjligheten till att på ett smidigt och effektivt sätt förflytta all trafik vid eventuellt datahaveri eller likande.

Frågan är dock hur säkerheten garanteras när det är en extern part som äger den faktiska hårdvaran? Hur kan företaget då veta säkert att information inte görs tillgänglig för någon obehörig? Det finns således anledning att föra en diskussion kring avvägningen mellan garanterad säkerhet och effektiva backup-system. För att Cloud Computing ska fortsätta ta mark behöver företagen som erbjuder sådana tjänster sannolikt utveckla säkrare miljöer med ökat kontroll. Ett förslag på en sådan lösning är så kallad Trusted Computing (en teknik utvecklad av Trusted Computing Group) och tillämpade kryptografiska tekniker (Chow, Golle, Jakobsson, Shi & Staddon, 2009, s. 5)

7.2 Hur länge spara data?

Personuppgifter får endast samlas in för särskilda, uttryckligt angivna ändamål vilka är berättigade (datainspektionen.se, 2011). De får endast användas för det syfte de ursprungligen samlades in för och enbart inkludera uppgifter som får anses nödvändiga för ändamålet. Som huvudregel gäller också att personen vars uppgifter registrerats ska ha lämnat sitt samtycke. För behandling av exempelvis personnummer finns ytterligare bestämmelser, där synnerligen motiverade skäl för lagring av uppgifterna måste finnas. När en personuppgift inte längre är nödvändig för det ursprungliga ändamålet skall den tas bort. (datainspektionen.se, 2011) Många företag har någon form av databas innehållandes kunddata, varför det kan vara av intresse att fundera kring denna lagstiftning. Sammanfattningsvis bör företaget säkerställa att de uppgifter

som samlas in faktiskt är nödvändiga för ändamålet samt be om medgivande från kunden när dennes uppgifter lagras.

Så snart en kunduppgift inte längre behövs ska den tas bort från registret. I vissa fall kan dock uppgifterna behöva bevaras en tid för att tillfredsställa annan lagstiftning, exempelvis kan detta gälla för bokföringsändamål. (datainspektionen.se, 2011) Det måste således beslutas hur länge data ska sparas, och då inte bara kunddata utan även annan information. En del av de lagringstider som gäller företagsinformationen är lagstadgade, så som exempelvis stora delar av den finansiella informationen. Det kan finnas andra data som ett företag kan ha intresse av att spara en längre tid, inte minst om det finns anledning att räkna med fortsatta kundkontakter under en lång tid framöver. Det är dock inte bara lagringstiden som måste bestämmas, utan även i vilket format data ska lagras, i och med att sådant som finansiell information och information kring kundstocken får ses som affärshemligheter. Det är således upp till varje företag att fundera kring om all data ska krypteras eller ej (se avsnittet om kryptering) samt hur länge lagrad data ska bevaras.

8 Hemsidan

Vad gäller IT- och datarelaterade krav inom värdepappersmarknaden är det egentligen endast hemsidan som givit något nämnvärt utrymme. I och med Internets ständigt ökade betydelse ökar dessutom vikten av företagens hemsidor som informationskällor.

8.1 Finansiell information

I lagar och regler betonas vikten av att på hemsidan presentera finansiell information och annan info som kan tänkas påverka aktiekursen. Denna information skall inte bara finnas tillgänglig ett flertal år, utan också presenteras på ett tydligt och lättillgängligt vis. Det är därmed av intresse att föra en generell diskussion kring hur företagets hemsida är uppbyggd samt dess innehåll, åtminstone den del som rör den finansiella informationen. Den information som enligt lagar och föreskrifter måste finnas tillgänglig på hemsidan är (NASDAQ OMX, 2011):

- All offentliggjord information (tillgänglig minst tre år)
- Aktuell bolagsordning
- Finansiella rapporter (tillgängliga minst fem år)
- Bolagets kalender (med uppgifter om viktiga datum så som offentliggörande av information, årsstämma osv.)

Till att börja med bör företaget fundera kring huruvida det är lämpligt att ha en separat sida för finansiell information och annat relaterat till företagsverksamheten (som exempelvis anställningsmöjligheter) eller om denna kan vara integrerad i den ordinarie webbsidan. När detta beslut är fattat är det av yttersta vikt att säkerställa att varje undersida fyller sitt syfte. Alla intressenter bör enkelt kunna finna den information de söker, det kan därför vara aktuellt att dela upp sidan utifrån exempelvis pressmaterial, finansiella rapporter och så vidare. För att ytterligare förenkla för intressenter bör en bra sökfunktion finnas, vilken täcker in all information som finns lagrad på webbsidan. Annat som kan vara av värde för intressenter är ett nyhetsflöde på förstasidan, vilket inkluderar alltifrån marknadsnyheter och finansiella rapporter till pressreleaser, samt grafik vilken visar börskursen och historik kring denna. (Sandahl, 2011)

Slutligen bör sidan göras sökbar för botar, för att möjliggöra att informationen kan hittas av sökmotorer så som exempelvis Google.

8.2 Säkerhet

Utöver hur företagets hemsida är uppbyggd, för att göra viktig information lättillgänglig för intressenter, är det också viktigt att hemsidan är säker. Bland annat bör giltiga certifikat finnas och eventuell e-handel drivas på ett sätt som är tryggt för kunden. Det är också kritiskt för företaget att sidan är skyddad mot överbelastningsattacker, så kallade DoS-attacker, då dessa kan resultera i att företagets viktigaste kommunikationskanal, hemsidan, slås ut under en tid. Mer om hur DoS-attacker förhindras beskrivs i avsnittet om logiska intrång.

8.2.1 Allmänt

Som kund är det inte alltid helt lätt att säkerställa vem ägaren till en hemsida är, vilket ändå kan vara av yttersta intresse då någonting ska inhandlas via nätet. Framförallt vill kunden förmodligen veta vem den betalar till och huruvida transaktionen är säker eller inte. Ett sätt att möjliggöra identifiering av webbplatsens ägare är genom användandet av Secure Socket Layer

(SSL) certifikat.(directNIC, 2011, s. 4) Ett SSL certifikat har två funktioner. För det första används det för verifiering och bestyrkande av identitet, för det andra möjliggör SSL certifikatet kryptering (veriSign, 2010, s.2). Certifikatet utfärdas av en betrodd tredje part, en så kallad ”Certification Authority” (CA), vilken säkerställer personen eller organisationens identitet innan certifikatet utfärdas. Certifikatet innehåller sedan information så som vem ägaren är, vilken server certifikatet sålts till, när det såldes och när det går ut. Denna information kan sedan användas av kunden när denne vill säkerställa att webbsidan är den som avses besökas.(directNIC, 2011, s. 4) Det finns dock också säkerhetsrisker som är av intresse att hantera för företaget själva. Exempelvis bör inte känslig eller onödig data finnas lagrad på hemsida, då denna på så sätt riskerar att göras tillgänglig för obehöriga läsare. Exempel på sådana data är information relaterad till betalkort.(Watson Hall Ltd., 2009, s. 1) SQL-injektioner (som beskrivits tidigare) måste också omöjliggöras då dessa kan orsaka stor skada och dessutom är enkla för en attackerare att utföra.

8.2.2 E-handel

Då majoriteten av alla konsumenter som köper varor på nätet föredrar att betala online med kort (DIBS, 2010, s. 14) är det viktigt att företag med en e-handelsplats tillhandahåller säker kortbetalning. Det finns idag mängder med företag vilka säljer säkra betalningslösningar för onlineköp, så som exempelvis DIBS, Payson och Klarna. Samarbetet med ett företag som handhar själva betalningslösningen måste också inkludera korrekt hantering av kvitton och fakturor.

I och med det ständigt växande antalet webbsidor vilka erbjuder varor till försäljning ökar konkurrensen och därmed kraven på de befintliga aktörerna. Webbplatsen måste finnas ständigt tillgänglig och kunden tolererar inte att den ibland ligger nere. Prissättningen måste vara tydlig, precis som vilka kostnader som tillkommer, exempelvis i form av frakt och eventuell moms. Det måste också tydligt framgå vem eller vilka som ligger bakom sidan, samt kontaktuppgifter till dessa.(Sandahl, 2011)

9 Hur nå bättre säkerhetsrutiner?

Det finns ett ord som ständigt återkommit i denna uppsats: Policy. Ett viktigt första steg mot en säker IT-hantering är att sätta upp mål och skapa en säkerhetspolicy. Denna bör vara så enkel som möjligt för att på så sätt göras lättillgänglig för anställda. Säkerhetspolicys skräddarsys efter företagets behov, men bör bland annat innehålla sådant som information om intrångshantering, både vad gäller hur upptäckt av sådan rapporteras och rutiner för hur företaget arbetar vidare. Det är av yttersta vikt att bevis inte går förlorade vid ett dataintrång. Platsen för intrånget ska betraktas som en brottsplats och händelser som skedde före, under och efter själva intrånget måste dokumenteras. Detta inte bara för en eventuell brottsutredning, utan även för att möjliggöra att lära sig från det inträffade och därmed minska risken för att det händer igen. Det är därför viktigt att hålla tillbaka impulser att starta om systemet för att få det rullande snarast möjligt. För att lyckas motstå sådana impulser krävs rutiner. Sådana tas lämpligen fram i med juridisk hjälp. Något annat som bör ingå i säkerhetspolicyn är rutiner för backup och återställning, då det krävs för att snabbt kunna återställa ett skadat system. Det kan exempelvis inkludera detaljer om vilka system som det är lönt att ta backup på, hur ofta detta ska göras, om det ska göras manuellt eller automatiskt och var dessa filer ska sparas (Crume, 2000, s. 57-58) Även hantering av skadlig kod bör ingå i säkerhetspolicyn. Skadlig kod kan innefatta alltifrån virus och trojaner till aktivt kontent (så som JavaScript). Dessa kan företaget till viss del skydda sig från med hjälp av antivirusskydd. Policyn bör således tala om vilken typ av skydd som ska finnas och hur ofta det ska uppdateras. Det är också viktigt att ta itu med lösenordsfrågan. Om företaget beslutar sig för att använda vanliga, textbaserade lösenord istället för exempelvis smartcards och liknande, måste det finnas regler för hur dessa lösenord ska utformas, för att nå en lägsta acceptabel standard. Vad gäller lagring och överföring av data måste kryptering diskuteras. Vad ska krypteras? Och hur säkra nycklar ska användas? Hur ska data kunna återställas om en nyckel går förlorad? (Crume, 2000, s. 59-61)

Det finns enkla rutiner som kan hjälpa företaget att förbättra sin säkerhetsnivå:

1. Identifiera strategisk och kritisk information vad gäller nödvändiga tillgångar, samt utifrån vad som krävs för att hålla den vardagliga verksamheten rullande. Se till att skydda dessa med olika medel och resurser
2. Installera någon form av IDS för att kunna monitorera eventuell fientlig trafik
3. Sätt upp responsteam och responsplan
4. Ta fram regler för inkommande trafik
5. Blockera IP adresser med misstänksamt ursprung
6. Sätt upp en heltäckande kontinuitetsplan som omfattar nätverk, mjukvara, system osv.
7. Ta fram plan för hantering av risker vilka ej kan åtgärdas för tillfället
8. Informera anställda om risker kopplade till bilagor som mottas via e-post
9. Skapa rutiner för patchhantering av virusskydd, speciellt för bärbara datorer uppkopplade mot modernätet
10. Ta fram rutiner för att snabbt och effektivt avsluta konton och behörigheter då en anställd slutar, både vad gäller att komma åt system, nätverk och lokaler.

ISO/IEC 27003 definierar en process med mått och steg som leder till framtagandet av policys utifrån en verksamhets- och nulägesanalys. (Heickerö & Larsson, 2008, s. 112-117).

- Först och främst görs en verksamhetsanalys, vilken bör vara övergripande och tidsbegränsad. Denna ska beskriva organisationens kärnverksamhet, speciellt i relation till omvärlden. Vidare ska huvudprocesser och relevanta funktioner åskådliggöras. De identifierade processerna och funktionerna ska därefter klassificeras utifrån krav på tillgänglighet, riktighet och sekretess och därefter prioriteras.
- Verksamhetsanalysen efterföljs av en nulägesanalys, vilken avser visa på hur informationssystemet bör se ut i form av policys och riktlinjer. I nulägesanalysen identifieras viktiga processer, speciellt de kritiska. Vidare görs en analys av hur processerna fungerar i dagsläget utifrån aspekterna tillgänglighet, riktighet och sekretess. Brister bör prioriteras och åtgärdas snarast.
- Nästa steg är en riskanalys vilken ska ligga till grund för framtida formulering av önskade säkerhetsnivåer. I analysen inventeras viktiga processer och verksamhetsstrukturer, utifrån vilka en konsekvensanalys görs. Denna ska formulera vilka hot specifika händelser kan resultera i och hur detta påverkar verksamheten. Hantering av uppenbara brister som upptäcks ingår inte i informationssäkerheten, men bör hanteras av annan resurs.
- Efter att riskanalysen är slutförd är det dags att ta fram en policy för informationssäkerhetsarbetet. Policyn skrivs utifrån det data som inhämtats i de tre tidigare genomförda analyserna. Även konsekvenser för att inte följa policyn ska uttryckas.
- Slutligen skall utformning av regelverk och anvisningar ske. Detta regelverk bör innehåla riktlinjer och anvisningar, vilka ligger till grund för hela det fortsatta säkerhetsarbetet. Både mål och hur dessa ska uppnås ingår lämpligen i dokumentet. De ansvariga för arbetet måste säkerställa att dessa regler successivt implementeras i organisationen.

10 Slutsats och Framtida Forskning

Konstateras kan, att bristen på reglering kring data och IT i samband med börsnoteringar är anmärkningsvärd. Det finns således ett ytterst begränsat antal regler som företag måste ta hänsyn till gällande just detta område. Däremot finns det krav på noggrann informationshantering. IT-säkerhet handlar trots allt om att skydda data, alltså den information som finns lagrad elektroniskt. Denna information är ofta värdefull för företaget och ska således skyddas på samma sätt som andra tillgångar. När diskussioner om IT-säkerhet förs är det viktigt att ha i åtanke att ingen lösning är fullständig. Det som ska diskuteras är därför hur säker en lösning är relativt en annan, inte hur säker en lösning är. Nedan presenteras två tabeller vilka sammanfattar de viktigaste slutsatserna från detta arbete. Den första tabellen gäller de faktiska krav som finns på företag i samband med börsnoteringar, samt hur dessa kan mötas. Den andra tabellen innehåller istället IT- och datarelaterade risker som kan vara intressanta för ett företag som skall börsnoteras att fundera kring.

10.1 Lagar och krav

Problematik	Kommentar	Lösning
Transparens vs. Sekretess	Företaget måste följa lagar gällande sekretess strax innan finansiella rapporter lämnas ut, utan att riskera förtroendekris till följd av bristande information.	Ledningen tillsammans med informationsansvariga och ekonomiavdelningen bör ha tydliga rutiner för att ta fram rapporter och lämna ut information. Lämpligen bör företaget öva sig på detta redan innan börsnoteringen.
Känslig information kan läcka ut	Kurskänslig information kan läcka ut till obehörig part, vilket kan leda till icke rättvis handel.	Det måste finnas rutiner för snabbt offentliggörande av information. Ju snabbare företaget kan sprida informationen som läckt ut till obehörig, desto mindre skada skedd
Loggbok	Alla börsnoterade företag måste föra loggbok över vem som delgetts känslig information och när	Loggboken bör omfattas av samma regler och föreskrifter som företagets redovisningshandlingar vad gäller förvaring, åtkomst och säkerhet. En policy bör också införas angående vem som får editera/läsa loggboken (detta kan kontrolleras med hjälp av digitala signaturer)
Hemsidan	Det finns ett antal krav på information som ska finnas på hemsidan	På hemsidan måste följande information finnas: • All offentliggjord information • Aktuell bolagsordning • Finansiella rapporter • Bolagets kalender Det är också lämpligt att ha ett certifikat för att tydliggöra vem som ligger bakom webbsidan, samt tjänst för säkra onlinebetalningar om webbshop finns.

10.2 IT- och datarelaterade risker

Problematik	Kommentar	Lösning
Riskanalys	Företaget bör göra en riskanalys redan innan det drabbas av några missöden, för att kunna prioritera säkerhetsnivåer för information och på så sätt skydda denna. Kostnaden för skydd bör vägas mot kostnaden för intrång.	• Vilka resurser måste skyddas? • Från vad/vem? • Vilken är kostnaden vid intrång? • Vilken är kostnaden för att skydda resurserna? • Vilken är sannolikheten för intrång?
Förlorad data riskerar företagets framtid	De flesta företag som förlorar viktig data drabbas hårt av detta	Kombinera backup (för kortsiktiga behov) och arkivering (för långsiktiga behov). Även databaser behöver tas backup på. En avvägning bör då göras mellan hur länge databasen kan ligga nere mot hur ofta backup ska tas.
Brandvägg är en bra början	Att investera i en brandvägg är en bra början för IT-säkerheten, men det är viktigt att tänka på att brandväggar inte stoppar virus.	En brandvägg kan bland annat användas för att isolera det interna nätet från andra nätverk, eller för att isolera en del av det interna nätverket. Lämpligen kompletteras brandväggen med ett antivirusskydd.
Kryptering	Kryptering kan användas för att skydda både lagrad data och data under överföring	Krypteringsalgoritm bör väljas utifrån företagets behov.
Lokaler	Se till att obehöriga inte får tillgång till känsliga delar av lokalerna	Inför strikt in- och utpasseringssystem och placera faxar/printers så att besökare inte ges naturlig access. Servrar placeras med fördel i separat byggnad dit endast fåtal har tillträde.
Vid stort databeroende	Vissa företag är extra beroende av tillgång till dess data, vilket då måste hantetras	En kostsam men mycket effektiv lösning är att ha en speglad datorhall. En billigare lösning är att ha dubbla nyckelkomponenter i systemen.
Laptops/USB	Bärbara enheter löper större risk att bli stulna/borttappade än stationära	Använd program som försvårar tillgång till data för obehörig. Affärshemligheter bör aldrig förvaras på bärbara enheter. För att säkerställa detta bör en policy kring bärbara enheter införas.
E-mejl	Företag eftersträvar möjlighet att skicka mejl konfidentiellt, med ändpunktsverifiering samt meddelandeintegritet	För att åstadkomma detta kan kryptering med symmetrisk nyckel användas i kombination med digitalt signerade hashfunktioner. Säkerheten bygger då på att nycklar bytts på säkert vis.
VoIP	Kan användas för att sänka kostnader, framförallt vis utlandssamtal, samt för att kunna	Var medveten om att det finns många säkerhetsrisker med VoIP! Som en början för att identifiera dessa kan

	dokumentera samtal	program användas för att scanna systemet på jakt efter säkerhetsbrister. Även kvalitetsbrister kan uppstå, men dessa minskar i takt med ökad bredbandshastighet
Smartphones	Risker ökar i och med att dessa enheter ofta används både i tjänsten och privat. Dock finns många fördelar, så som möjlighet att läsa e-post överallt.	Strikt policy bör införas gällande vilka användningsområden som är tillåtna för smartphones, samt vilken information som får finnas på dessa.
WiFi	Trådlösa nätverk underlättar ofta för företag, framförallt för besökare	Använd WPA2 för tillfredsställande säkerhet, undvik WEP! Inför policy kring vem som får använda trådlösa nätverk och hur.
Om intrång sker	Om faran är framme är det viktigt att hantera detta på rätt sätt	Det bör finas tydliga rutiner för hur intrång hanteras. En handlingsplan med bland annat info om vilka myndigheter som ska kontaktas, mallar för rapportering osv. bör tas fram. Detta för att snabbt kunna återställa säkerheten utan att förstöra bevis.
Insiderattack	En hacker behöver inte vara en extern person. Det måste således finnas skydd även internt.	Sätt upp interna brandväggar för att skydda känslig information. Se till att ta bort åtkomsträttigheter så snart en anställd slutar.

10.3 Framtida Forskning

Det kan vara av intresse att göra en motsvarande undersökning som denna, men vilken istället riktar in sig på mobilanvändningen. Det är idag relativt enkelt att hacka sig in i en mobiltelefon, inte minst om den använder WiFi, vilket många idag gör i och med smarta telefoners framfart. Om inkorgar är kopplade till mobiltelefonen finns då risk att en attackerare som inte lyckas hacka sig in i mejlen via datorn istället med enkelhet kan göra detta via mobiltelefonen.

Referenser

LITTERATUR

Beaver, K. (2010): "Hacking for Dummies, 3rd Edition", Wiley Publishing, Inc., Indiana
ISBN: 978-0-470-55093-9

Carr, J. (2009): *"Inside Cyber Warfare*", O'Reilly Media, Inc., Kalifornien
ISBN: 0-59680-215-3

Crume, J. (2000):*"Inside Internet Security – What Hackers Don't Want You to Know",* Pearson Education Ltd., London
ISBN: 0-201-67516-1

Grundvall, B., Melin, A. & Thorell, P. (2004): *"Vägvisare till börsen"*, Liber Ekonomi, Malmö
ISBN: 91-47-07528-7

Heickerö, R., & Larsson, D. (2008): *"Terror Online",* Conopsis Förlag
ISBN: 91-633-1842-3

Kurose, J. & Ross, K. (2010): *"Computer Networking – a top down approach"*, Pearson Education, Inc., Boston
ISBN: 0-13-136548-7

Mitrovic´, P. (2003): *"Handbok I IT-säkerhet, 3:e upplagan"*, Pagina Förlag AB, Göteborg
ISBN: 91-636-0796-4

Olsson, F. (2006): "*Säkerhet i Trådlösa Nätverk*", 4G Media
ISBN: 91-975710-0-8

Placera Media (2010): *"Börs Guide 2010:2",* Placera Media, Stockholm
ISSN: 91-978589-2-7

Sandeberg, af, C. (2001): *"Börsnotering",* Iustus förlag, Uppsala
ISBN: 91-7678-475-4

Sandeberg, af, C. (2001), *"Prospektansvaret"*, Iustus Förlag AB, Uppsala
ISBN: 91-7678-459-2

Sandeberg, af, C. & Sevenius, R., (2007): *"Börsrätt",* Studentlitteratur AB, Pozkal
ISBN: 978-91-44-04581-8

Shim, J., Qureshi, A. & Siegel J. (2000): *"The International Handbook of Computer Security",* the Glenlake Publishing Company, Ltd., Chicago
ISBN: 1-888998-85-7

Verizon Business (2011): *"2011 Data Breach Investigations Report"*

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Örtengren, T. (2007): *"Börsintroduktion på Stockholmsbörsen – noteringsprocessen och noteringskrav",* ur Sandeberg, af, C. & Sevenius, U.: *"Börsrätt",* Studentlitteratur AB, Polen
ISBN: 978-91-44-04581-8

ARTIKLAR OCH RAPPORTER

Botha, R. A., Furnell, S. M. & Clarke, N. L. (2008): *"From desktop to mobile: Examining the security experience"*
http://www.sciencedirect.com/science/article/pii/S0167404808001089

Chow, R., Golle, P., Jakobsson, M., Shi, E. & Staddon, J. (2009): *" Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control"*
http://www.eecs.berkeley.edu/~elaines/docs/ccsw.pdf

DIBS (2010): *"DIBS e-handelsindex Sverige 2010"*, En undersökning utförd av YouGov Zapera för DIBS Payment Services

directNIC (2011): *"SSL Certificates"*
http://www.directnic.com/help/guides/pdf/ssl_certificates.pdf

Elcomsoft Proactive Software (2007): *"Advantages and Disadvantages of EFS and Effective Recovery of Encrypted Data"*
http://www.elcomsoft.com/WP/advantages_and_disadvantages_of_efs_and_effective_recovery_of_encrypted_data_en.pdf

Eriksson, F. & Fogel, J. (2008): *" Encryption: Protection of Sensitive Information"*
http://www.idt.mdh.se/kurser/ct3340/archives/ht08/papersRM08/14.pdf

Finansinspektionen (2007a): *"Rapport 2007:11: Processen vid nyintroduktioner och emissioner"*
http://www.fi.se/Utredningar/Rapporter/Listan/Processen-vid-nyintroduktioner-och-emissioner-200711/

Finansinspektionen (2007b): *"Rapport 2007:12: Emissioner och nyintroduktioner – fungerar skyddet för investerarna?"*
http://www.fi.se/upload/20_Publicerat/30_Sagt_och_utrett/10_Rapporter/2007/Rapport2007_12.pdf

Finansinspektionen (2011): *"Vägledning 2011-01-14: Granskning av prospekt"*
http://www.fi.se/Regler/Vagledning/Prospekt/

Halpern, J. (2003)*: "IP Telephony Security in Depth"*, Cisco Systems
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.pdf

Hogben, G. & Dekker, M., ENISA (2010*): "Smartphones: Information security risks, opportunity and recommendations for"*

Kuhn, D. R., Walsh, T. J. & Fries, S. (2005): *"Security Considerations for Voice Over IP Systems - Recommendations of the National Institute of Standards and Technology"*
http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

Mansfield-Devine, S. (2009): *"Darknets"*
http://www.sciencedirect.com/science/article/pii/S135348581070115X

McGann, S. & Sicker, D. C., (2005): *"An Analysis of Security Threats and Tools in SIP-Based VoIP Systems"*
http://spot.colorado.edu/~sicker/publications/analysis.pdf

Online Trust Alliance (2011): *"2011 Data Breach & Loss Incident Readiness Guide"*
https://otalliance.org/resources/2011DataBreachGuide.pdf

Ponemon Institute (2011): *"The State of USB Drive Security - U.S. survey of IT and IT security practitioners"*
http://www.kingston.com/secure/PDF_files/MKP_272_Ponemon_WP.pdf

PWC (2011): *"Riskpremien på den svenska aktiemarknaden"*
http://www.pwc.com/sv_SE/se/publikationer/assets/pdf/riskpremiestudien-2011.pdf

Richardson, R. (2008): *"CSI Computer Crime & Security Survey"*
http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf

Siemens Enterprise Communications (2008): *"WLAN Security Today: Wireless more Secure than Wired"*
http://www.enterasys.com/company/literature/WLAN%20Security%20Today-Siemens%20whitepaper_EN.pdf

Tandeberg Data (2010): *"Guide to Data Protection Best Practices – A Tandeberg Data white paper on backup and archival storage best practices"*
http://www.exabyte.com/support/online/documentation/whitepapers/basicbackup.pdf

VeriSign (2010): *"Beginners Guide to SSL Certificates – Making the Best Choice When Considering Your Online Security Options"*
http://www.verisign.com/ssl/ssl-information-center/ssl-resources/guide-ssl-beginner.pdf

Watson Hall Ltd. (2009): *"Top 10 website security issues – the website security issues to tackle first"*
https://www.watsonhall.com/resources/downloads/top10-website-security-issues.pdf

WiFi Alliances (2005): *"Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise"*
http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf

Winencrypt (2009): *"USB and Flash drive security policy best practices checklist"*
http://www.winencrypt.com/downloads/resources/security-best-practices/WinEncrypt_usb_flash_drive.pdf

LAGAR, REGELVERK OCH BETÄNKANDEN

IK120X
Sara Klingberg

Brottsbalk(1962:700)

Europaparlamentets och rådets direktiv 2003/71/EG: *"Prospektdirektivet"*

Kommissionen Förordning (EG) nr 809/2004: *"Prospektförordningen"*

Kommissionen Förordning (EG) nr 211/2007: *"Ändring av Prospektförordningen"*

Lag (1991:980): *"Om handel med finansiella instrument"*

Lag (2000:1087) *"om anmälningsskyldighet för vissa innehav av finansiella instrument"*

Lag (2005:377) *"om straff för marknadsmissbruk vid handel med finansiella instrument"*

Lag (2007:528): *"Om värdepappersmarknaden"*

NASDAQ OMX (2008): *"Hantering av loggbok OMX"*

NASDAQ OMX (2011): *"Regelverk för emittenter NASDAQ OMX Stockholm"*

SOU 2006:50: *"En ny lag om Värdepappersmarknaden"*

AVHANDLINGAR

Delgado, V. (2010):*"Exploring the limits of cloud computing",* Magisteruppsats, ICT, KTH, Stockholm
http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/101118-Victor_Delgado-with-cover.pdf

Lindholm, V. & Westergren, A. (2002): *"Informationshantering i börsnoterade företag"*, Magisteruppsats, Ekonomiska Institutionen, Linköpings Universitet, Linköping
http://liu.diva-portal.org/smash/record.jsf?pid=diva2:19304

Nordhoff, M. (2006): *"Security Evaluation of SCTP",* Kandidatuppsats, Computer Networking Group, University of Duisburg-Essen, Essen
http://homepage.ruhr-uni-bochum.de/Michael.Nordhoff/SecEvalSCTP06.pdf

WEBBSIDOR

http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/hur-lange-far-personuppgifter-bevaras/#vadstardet, Datainspektionen: *"Hur länge får personuppgifter bevaras?",* information om personuppgiftslagen, åtkomst: 2011-05-05

http://www.fbi.gov/about-us/investigate/counterintelligence/business-brochure, FBI: *"Business Brochure",* säkerhetstips för företag, åtkomst: 2011-08-18

http://h41112.www4.hp.com/promo/obc/se/sv/business-it-advice/protect-your-business/how-to-keep-your-business-safe-online.html, HP: *"Hur arbetar företaget säkert online?"*, Tips från HP gällande hur företag kan förbättra sin IT-säkerhet, åtkomst: 2011-05-14

http://www.nasdaqomxnordic.com/about_us?languageId=3, NASDAQ OMX: *"Om NASDAQ OMX"*, historik om stockholmsbörsen, åtkomst: 2011-04-16

http://www.swedishbankers.se/web/bf.nsf/$all/2180C05EFB647D91C125760F003C46D5, Svenska Bankföreningen: *"Ordlista"*, ordlista över värdepappershandelsbegrepp, åtkomst: 2011-05-01

http://web.mit.edu/ist/isnews/v22/n04/220406.html, MIT: *"Safe Computing: Erase Data from Devices before You Sell or Recycle"*, tips från MIT om hur företag bör agera inför återvinning och försäljning av datorer och mobiltelefoner, åtkomst: 2011-08-18

INTERVJUER

Person X, VD, Företag nr 1, utförd 2011-05-16

Person Y, VD, Företag nr 2, utförd 2011-05-13

Jörgen Sandahl, VD WordOn, expert på onlinemarknadsföring och försäljning, utförd 2011-09-19

Appendix A

Nedan återfinns en checklista från Tandberg Data vilken kan hjälpa ett företag att skapa en backup- och arkiveringsplan för att säkra data och minimera kostnader (Tandberg Data, 2010, s.12)

- Network data backup plan—types of data
  - Data files
  - Operating systems
  - Databases
  - Application programs
  - Application settings
  - Windows device drivers
  - Network settings
- What data can be archived to tape to free up disk storage resources, and reduce running costs
- How long must data be archived?
- Quantity of data to be backed up
  - How much data will typically be stored in a full backup?
  - How often will a full backup be done?
  - How much data will typically be stored in a partial backup?
  - How often will a partial backup be done?
- End user desktop and notebook backup scheme
  - Desktop, notebook environments
  - Application programs
  - Application settings
  - Data files
  - Address books
- End user data backup recommendations (copy to network first)
- End user data recovery checklist—what to do and what not to do when suspecting data loss
- Network administrator data recovery checklist
- Prioritization: Which data to back up first
- Data backup strategy (schedule of full and partial backups)
- Choice of backup hardware with an eye to automation
- Choice of backup software
- Archive strategy (on-site and off-site backup storage locations)
- Tape management (how many tape sets; rotation plan)
- Restore process actually tested prior to needing it
- Capital investment budget (hardware, software, implementation)
- Operating budget—recurring costs

Appendix B

Tabell over svagheter I VoIP ((McGann & Sicker, s. 2).

Layer	Attack Vector	Confidentiality	Integrity	Availability
Network Interface	Physical Attacks	x		x
	ARP cache	x	x	x
	ARP flood			x
	MAC spoofing	x	x	x
Internet	IP Spoofing			
	Device	x	x	x
	Redirect via IP spoof	x	x	x
	Malformed packets	x	x	x
	IP frag	x	x	x
	Jolt			x
Transport	TCP/UDP flood			x
	TCP/UDP replay	x	x	
Application	TFTP Server insertion		x	
	DHCP starvation			x
	ICMP flood			x
	SIP			
	Registration Hijacking	x	x	x
	MGCP Hijack	x	x	x
	Message modification	x	x	
	RTP insertion			
	Spoof via header	x	x	x
	Cancel/bye attack			x
	Malformed method			x
	Redirect method	x		x
	RTP			
	SDP redirect			x
	RTP payload			x
	RTP tampering	x	x	x
	Encryption	x	x	x
	Default configuration	x	x	x
	Unnecessary services	x	x	x
	Buffer overflow	x	x	x
	Legacy Network	x	x	x
	DNS Availability			x

TRITA-ICT-EX-2011:235

www.kth.se