SÄRTRYCK UR CIO SWEDEN.
Publikationen utgiven av IDG.
Världens största utgivare av datorrelaterad fackpress.

IT DUE DILIGENCE – *eller hur du undviker att köpa grisen i säcken*

Inför uppköpet av ett belgiskt företag genomfördes en traditionell due diligence. Trots detta gick allt fel. It-kostnaderna sköt i höjden, företaget förlorade marknadsandelar, var nära konkurs och var tvunget att skriva av nästan hela uppköpet. Här beskriver vi vad som gick snett.

AV MIKAEL SIMOVITS

MIKAEL SIMOVITS
är konsult i egen regi med forskar- och kryptologbakgrund och har jobbat med it-säkerhet sedan 1994.

DET HADE PRECIS BLIVIT VÅR. Företagets ledningsgrupp var samlad i ett inte allt för charmigt konferensrum. Förutom ledningsgruppen var revisorer, jurister och konsulter från ett av de stora revisionsföretagen närvarande – samt några oberoende finansiella rådgivare. Det var dags att presentera resultatet av en utförd due diligence av ett belgiskt bolag. Prislappen var upptrissad, men förståsigpåare ansåg att det belgiska bolaget genom sin molntjänst bröt ny mark. Dessutom var konkurrenterna också intresserade.

Efter dragningen var alla eniga om att affären var bra. Den skulle ge ett välbehövligt tillskott i produktportföljen som ökade företagets marknadsandelar och gav en skjuts ut på nya marknader. Att komma över en färdig produkt med ”noll” dagar till marknad vara värt den halva miljard de belgiska entreprenörerna krävde för sitt företag.

Trots detta gick allt fel. Företaget förlorade marknadsandelar till en grad att det var nära konkurs och it-kostnaderna sköt i höjden. I denna artikel ska vi ta en titt på vad som hände – och vad man borde ha gjort annorlunda.

Vad är due diligence?

Som nämnts ovan föregicks köpet av det belgiska företaget av en due diligence, vilket fritt kan översättas till duglighetskontroll eller ”företagsbesiktning”. I samband med en företagsfusion eller ett uppköp åsyftar due diligence en metod för att analysera uppköpskandidaten ur alla tänkbara vinklar för att bedöma affärens risk – vilket självklart är lättare sagt än gjort. De största utmaningarna är att bestämma *vad som ska kontrolleras* och *hur lång tid kontrollen ifråga får ta*. Det senare dilemmat innebär att om perioden är för kort kommer resultatet med största sannolikhet att bli missvisande och är tiden för lång kan händelser göra att någon av parterna tröttnar och ångrar sig.

Om vi betraktar frågan om vad som måste besiktigas, så omfattas vanligtvis ett flertal områden såsom:

- ekonomi/finans
- juridik
- marknad
- personal/lönesättningar/förmåner
- ledning/styrning
- skattefrågor
- miljö
- It
- produkt (teknik)
- patent/varumärke samt övriga produktskydd
- risk och försäkring

Det är företagets ledning som bestämmer kontrollmål och omfattning av besiktningen – och det är en svår avvägning. I synnerhet när det gäller it-risker eftersom det är något många företagsledningar fortfarande har bristfälliga kunskaper om. Normalt sett utgör it och teknik mellan fem och tio procent av vad som bör kontrolleras. Här gäller det att verkligen se upp, för som vi snart ska se kan det bli dyrt om man slarvar.

KONTROLLMÅL

Kontrollmålen för besiktning av it-stödsystem och besiktning av it som produkt skiljer sig åt, och måste uppmärksammas vid en genomgång. Oftast glider dessa områden in i varandra.

IT-STÖDSYSTEM

Inventering: Vilka system, vilken hårdvara och vilken mjukvara finns? Är systemen säkra, fungerar de korrekt och vem äger olika delar av it-miljön?

Styrning: Hur bra stödjer it verksamheten, och hur beroende är verksamheten av it? Vilka behov av förändringar finns, hur styrs förändringsprocessen inom företaget och hur mäts företagets it-relaterade verksamhetsmål?

Strategi: Hur är det tänkt att it-miljö och personal ska utvecklas för att möta framtida behov? Vilka produkter och vilka leverantörer ska användas på sikt?

IT-PRODUKT

Inventering: Produktens funktionalitet utifrån kundens synvinkel

Styrning: Roadmap för produkten i form av rättningar och ny funktionalitet som ska införas i framtiden

Strategi: Utvecklingsprocesser, nyckelpersonsberoenden och skydd av produkt (patent)

Vid dragningen av det belgiska bolagets due diligence-rapport hade endast två av de närvarande teknisk bakgrund: it-chefen och it-revisorn som lett den it/tekniska genomgången. På det tre timmar långa mötet diskuterades it och teknik endast under cirka femton minuter. It-revisorn presenterade då vilken metod som använts och de iakttagelser som gjorts. Det som iakttogs var följande:

- **Det belgiska företaget hade två nyckelpersoner** som måste tillvaratas. Dessa ledde all it-relaterad hantering, internt såväl som externt.
- **Man hade en uttalad strategi** att bygga allt på öppen källkod.
- **Den tekniska dokumentationen** var bristfällig och utdaterad.
- **Den enda programvara som krävde licens** var Windows-klienter och Microsoft Office. Övriga maskiner var baserade på öppen källkod.
- **Serverparken** bestod av fyrtio servrar i produktionsmiljön, och hårdvaran var nyligen utbytt.
- **Ekonomisystemet** var planerat att bytas ut inom ett år.
- **Viss personalomsättning på it-sidan** hade noterats.

Det som sades mellan raderna var att it-miljön inte hade hängt med i företagets snabba expansion, och att verksamheten fortfarande hade mycket av ”entreprenörsanda”. Men det var inte riktigt något som någon tog in – och ingen insåg vidden av problemet. Köpet genomfördes.

En första indikation på att allt inte stod rätt till kom redan vid integrationen av kontorsnätverken. Det som noterades var att det saknades klientstandard på arbetsstationer och laptops. I princip hade varje användare en unik pc och hälften av datorerna hade köpts hos en lokal tv/radio/dator-handlare i kvarteret. Dessutom saknades en trovärdig infrastruktur för fillagring och e-post.

För att överhuvudtaget kunna kopplas ihop med moderbolaget fick hela nätverket uppdateras. Nya datorer köptes till varje anställd och nya servrar för behörighetshantering, filhantering och e-post i kontorsnätet införskaffades. Notan slutade på fyra miljoner kronor.

Allvarliga it-brister upptäcks

Men det var inte allt. Vidden av bristerna i det belgiska företagets molntjänst uppdagades lagom till semestern, inför integrationen mot moderbolagets molntjänster. Bristerna var allvarliga och berörde tre områden; s*kalbarhet och prestanda, integration* samt *plattform.*

Skalbarhet och prestanda: Det belgiska företagets lösningsarkitektur byggde på att varje ny företagskund fick en egen server. Här ingick webb, applikation och databas. Varje server var skild från övrig infrastruktur och nyttjade bara 20–30 procent av sin kapacitet. Dessutom var varje server en single point of failure, det vill säga felkritisk. En krasch skulle innebära minst 1–2 dagars nedtid för den drabbade kunden.

Det visade sig också att en orsak till att varje kund fick en egen server var att lösningen saknade adekvat behörighetssystem. Provanvändare och små kunder delade på en server och man kunde genom manipulationer i anropssträngen komma åt andra kunders data.

Integration: Integrationen blev ett problem i och med att varje kundlösning var unik. Ett helt nytt integrationslager var tvunget att byggas för att integrera lösningarna.

Plattform: Många av mjukvarorna var utdaterade. Plattformens konstruktion och designval var odokumenterade och endast kända av nyckelpersonerna. Efter en genomgång framkom orsaken till att senare versioner inte användes: Den egenutvecklade mjukvaran fungerade helt enkelt inte i senare versioner av plattformen.

Lösningen hade nått toppen av sin funktionalitet, det var omöjligt att bygga in funktioner som återfanns i konkurrenters lösningar utan att bygga om allt från grunden.

”Det är företagets ledning som bestämmer kontrollmål och omfattning av företagsbesiktningen, och det är en svår avvägning ...”

De direkta affärsmässiga konsekvenserna blev att företaget tappade marknadsandelar till konkurrenter och förloarde möjlighet att följa med utvecklingen, samtidigt som man saknade kapital för att utveckla lösningar.

När tekniken förbises

Det var inte första eller sista gången ett företagsköp går fel. Ett klassiskt varningsexempel är *ABB:s* köp av *Combustion Engineering*, ett företag med stora skulder och överhängande asbestål, som höll på att stjälpa ABB i början av 2000-talet. Lärdomen här var att det är viktigt att ha sitt på det torra vad gäller ekonomi och juridik och metodiskt se över den typen av risker. Det har de flesta insett, men som nämnts underskattas ofta risker knutna till teknikval. Hur det kan slå ska vi visa nedan genom att analysera några nyckelfaktorer vid en en traditionell due diligence för att sedan översätta resonemanget till it. De vi tittar på är:

- Beställarens kompetensprofil
- Definition av områden och djup
- Tid och kostnad för utförandet
- Metod för utförandet
- Bemanning

BESTÄLLARENS KOMPETENSPROFIL: Beställare av en due diligence brukar vara företagsledningar och/eller riskkapitalister. De har oftast en ekonomisk bakgrund varvid tyngdpunkten ligger på marknad, juridik och ekonomi. Beställaren är helt enkelt mest intresserad av vilken marknadspotential ett företag eller en produkt har, vilken form av strukturkapital som erhålls vid köpet, företagets finansiella data och/eller om det finns juridiska hinder för köpet.

DEFINITION AV OMRÅDEN: Ett stort antal områden måste undersökas för att få en helhetsbild av ett företag. Områdena måste prioriteras gentemot varandra och anpassas för den verksamhet som ska granskas. It och teknik är högre prioriterat då det gäller ett teknikföretag än om det handlar om ett mer traditionellt producerande företag.

TID OCH KOSTNAD FÖR UTFÖRANDET: Det är mycket som ska undersökas och en due dilligence kan endast utföras under en kort period. Det begränsar självklart djupet vid utförandet och kvaliteten på slutsatserna. Resultatet måste accepteras utifrån dessa villkor.

METOD FÖR UTFÖRANDET: För att vara så effektiv som möjligt under en kortare tid utgår besiktningen oftast från checklistor. På så sätt uppnås spårbarhet på vad som kontrollerats om diskussioner skulle uppkomma efteråt. Normalt är cirka fyrtio kontrollpunkter avsedda för it och teknik av totalt cirka 750 kontrollpunkter för hela verksamheten. Eftersom ingen verksamhet är helt lik någon annan är checklistorna oftast generella till sin natur och tar inte hänsyn till speciella egenheter.

BEMANNING: Oftast får företag som är specialiserade på M&A (Mergers & Acquisitions) uppdraget att leda samt utföra hela due diligence-uppdraget. Det innebär att projektet ofta bemannas med revisorer, it-revisorer, jurister och konsulter med liknande kunskapsprofiler. Den totala it-kunskapen kan jämställas med den vid en it-revision.

Om vi beaktar ovanstående ser vi snabbt att ett traditionellt due diligence-förfarande har en tendens att lägga tyngdpunkten vid områden som företagsledningen och det utförande företaget behärskar. Om både beställaren och utföraren saknar it-kunskap kan väsentliga risker förbises, som i faller med köpet av det belgiska företaget.

När tekniken beaktas!

En teknisk due diligence kan genomföras med samma utgångspunkter som en vanlig, men med större tonvikt lagd på frågor om teknikval, teknisk design och tekniska begränsningar i det undersökta företagets produkter.

Om en CIO är med i beslutsfattandet, vilket ca 70 procent av CIO:erna brukar vara (enligt amerikanska CIO Magazines undersökning ”State of the CIO 2010”), så finns det en chans att kunna styra upp den tekniska delen vid en due dilligence på det sätt som krävs. Låt oss se på nyckelfaktorerna igen, när vi lagt större vikt vid it.

BESTÄLLARENS KOMPETENS: Beställaren för en teknisk due diligence måste förstå tekniken som ska granskas.Han eller hon ska själv förstå it och konsekvenserna av olika användningsområden och bör gärna ha erfarenhet som systemarkitekt, programmerare eller systemtekniker. Detta för att förstå vad som ska granskas och snabbt kunna besluta om fokusområden. CIO, eller den person CIO har delegerat ansvaret till, bör lämpligen axla rollen som beställare och för definitionen av kontrollmål.

DEFINITION AV OMRÅDEN: En CIO bör driva frågan att en tekniska due diligence genomförs och se till att rätt resurser blir tillsatta för att genomföra granskningarna.

TID OCH KOSTNAD FÖR UTFÖRANDET: Samma restriktioner som för traditionell due diligence.

METOD FÖR UTFÖRANDET: Befintliga checklistor ska användas, eftersom informationen som hittas genom dessa fortfarande är intressant och relevant vid ett företagsuppköp. Bäst är dock att välja en bottom-up metod med förutsättningslösa teknikgranskningar av målmiljön. Följande frågor borde till exempel ha ställts i det aktuella fallet med det belgiska företagsköpet:

- **Kan en annan part ta över** och förstå källkoden?
- **Kan lösningarna integreras** mellan de båda företagen, och vad måste i så fall göras?
- **Vilken funktionalitet** går det att utöka lösningen med på kort och lång sikt?
- **Var finns flaskhalsarna** avseende prestanda?
- **Finns det arkitekturella hinder** som hindrar införandet av ny funktionalitet?
- **Hur är säkerheten** löst tekniskt?

BEMANNING: De bästa personerna för att göra denna typ av genomgångar hittas i tekniska konsultföretag. Dessa personer bör ha en erfarenhet av liknande plattformar och kunna sätta detta i relation till projektkostnader, förvaltningskostnader samt verksamhetsmål. Naturligtvis kan egen personal användas, men risken är att den sätter sina personliga mål före företagets och anpassar sig efter den stämning som finns i företaget och omedvetet/medvetet blundar för eventuella problem. Fördelen är förstås att den egna personalen känner till sin tekniska lösning och dess kvalitet. Egen personal kan användas om den känner att den kan uttala sig om tekniken utan att på något sätt riskera sin personliga situation i företaget.

Att köpa ett företag utan teknisk due diligence kan liknas vid att köpa en begagnad bil utan att kolla med verkstaden. Än är det en bra bit kvar. Utvärderingar vittnar om misslyckanden i 40–50 procent av fallen.]

KONTROLLPUNKTER VID TEKNISK DUE DILIGENCE

Typiska kontrollpunkter vid traditionell teknisk due diligence

1. Nyckelpersonsberoende för utveckling och drift av system
2. Ägandeförhållanden avseende källkod
3. Ägandeförhållanden avseende hårdvara
4. Kvalitet på systemdokumentation
5. Ålder på hårdvara och inköpta system
6. Konsultföretag som utvecklat koden, samt dessa företags stabilitet, källkodsdeponering
7. Inventering av mjukvarulicenser
8. It-organisation och rapporteringsstruktur
9. Finns det framtidsplaner/ roadmaps?
10. Bemanning av utvecklingsteam
11. Finns utvecklingsprocess dokumenterad?
12. Stämmer designdokumentation med verkligheten?
13. Teknisk support, ansvar och bemanning
14. Inventering av patent, licenser och patenttvister
15. Säkerhet
16. Verksamhetskritiska system

För en grundligare due diligence, lägg till:

17. Kodkvalitet och kodstandard
18. Arkitektur på produkter och lösningar avseende funktionalitet, skalbarhet och integration
19. Plattformsval
20. Systemadministration

OM DU VILL LÄSA MER

Artikeln är ett kondensat av erfarenheter från flera olika fusioner. Om man är intresserad att läsa mer är en googling på ”misslyckade fusioner” ett bra insteg. Annars rekommenderas följande böcker:

”LIVSFARLIG LEDNING – historien om kraschen i ABB” av Bengt Carlsson
”DUE DILIGENCE: Planning, Questions, Issues” av Gordon Bing
”CHECKLISTS FOR DUE DILIGENCE” av Peter Howson