EN VD:s GUIDE TILL INFRASTRUKTUR I MOLNET

15 Frågor som din IT-chef borde besvara redan idag

safespring

Vem har nytta av denna eBook?

Som VD har du ansvar för att säkerställa bolagets konkurrenskraft, minimera risker och öka effektiviteten i bolagets processer och rutiner. Allt fler företag överväger idag att investera i eller outsourca sina infrastrukturtjänster till en molnleverantör.

Men området är stort och alternativen många. Ska du outsourca hela eller vissa delar av din serverpark? Är det datalagring och backuplösningar som måste moderniseras?

Som VD kan du inte vara expert på dessa områden, men med hjälp av nedanstående frågeguide kan du få hjälp att formulera rätt frågor till din IT-chef, för att säkerställa att ni har bred marginal mot potentiella risker samt att ni har en effektiv infrastruktur.

safespring

Vilka fördelar finns det i att outsourca sina infrastrukturtjänster till molnet?

Många som driver en egen infrastruktur har en betydligt högre kostnadsnivå än nödvändigt. Det är fysiskt omöjligt att skala ned en investering, så har man varierande behov av kapacitet måste man dimensionera för maxbelastning. Detta leder till att man många gånger har en överkapacitet som man betalar dyrt för. Det finns ofta inget egenvärde för organisationer att ha en egen infrastruktur. Istället är i grunden den **flexibilitet** och **skalbarhet,** vad gäller både teknik och pris, som molntjänster innebär naturligt intressant för de flesta. Flexibiliteten ifrån en modern plattform ger användaren möjlighet att skala upp och ned resurser samt experimentera i högre grad. Forsknings- och utvecklingsprojekt kan snabbt allokera resurser och vid produktionssättning kan man få en betydligt snabbare time-to-market. De vanligaste drivkrafterna för att köpa infrastruktur som tjänst är ökad effektivitet i leveransen, snabbare innovationstakt, snabbare time-to-market och högre feltolerans. Samtidigt får man billigare IT resurser och vid rätt val av leverantör, automatiserade öppna plattformar.

Dels finns det en **kommersiell** fördel i det att man enbart betalar för de resurser man faktiskt använder. Om man inte vill oroa er för sin egen infrastruktur så är detta också en fördel som kommer med outsourcing av infrastrukturtjänsterna. Den **operationella** kostnaden ersätter de stötvisa investeringskostnaderna och kan följa med behoven på ett mer praktiskt sätt.
När du börjar använda molntjänster kommer du att spara tid vilken istället kan läggas på att utveckla ditt företag i rätt riktning och i de frågorna ni faktiskt brinner för. Dessutom kan du förlita dig på att din data finns samlad i datacenter av **modern standard**, kapaciteten uppdateras hela tiden utan att du själv måste byta ut hårdvaror varje år.

Om man går hela steget och implementerar en “cloud native-plattform” för applikationer, såsom *Kubernetes*, i sin infrastrukturtjänst kan man göra oerhörda vinster vad det gäller flexibilitet och skalbarhet.

När ska man börja fundera på att outsourca sina infrastrukturtjänster?

Ett företag behöver vid något tillfälle ta beslut om när det är dags att gå över till en **ny generation** teknik- och IT-stöd. Dessa uppgraderingar kommer med jämna mellanrum.

De flesta företag brukar resonera som så att de inte vill vara bland de första som provar den nya tekniken. Då finns risken att de får hantera ofärdiga IT-lösningar. Däremot vill företagen heller inte vara bland de sista eftersom övriga branschföretag, som redan tagit till sig den nya teknologin, då kommer att ha en **operativ konkurrensfördel** tills det att ert bolag också investerar i likvärdig teknologi. Därför är det viktigt att ta steget ungefär samtidigt som dina branschkollegor.

Var bör man börja om man vill migrera till molnet?

Klassificera först vilka system ni sitter på och hur ni hanterar er affärsdata idag. Vilken typ av system och data passar bäst att migrera till molnet och vilken är det bra att ni behåller hos er själva? **Olika system har olika behov**. Säkerhet och lagstiftning är viktiga faktorer som bör vara en del av denna värdering.

Styrkan med molntjänster är att man kan börja med ett separat system för att sedan växa in i den plattform man har valt. Exempel på system som kan passa bra att flytta ut är de vars belastning varierar eller växer raskt. Det är viktigt att inte gapa för stort med en gång, utan stegvis sätta sig in i möjligheterna och teknologin medan man bygger kompetens och erfarenhet.

4 Vad finns det för risker med att outsourca sina infrastrukturtjänster?

Många ser en flytt till molnet som ett stort projekt där allt skall flyttas på en gång. Det bästa är att först ta fram en strategi där ni identifierar de system som passar för flytt ur ett säkerhets- och skalfördelsperspektiv och börjar med dem.

Ett vanligt fel köpare av infrastrukturmolntjänster gör är att bara gruppera sina tjänster på server-nivå och migrera sina servrar rätt in i tjänsten utan anpassning. De stora fördelarna finns att tillskansa sig om man **designar sina applikationer för molnet**, med separation mellan de olika delarna i applikationerna, vilket gör att det blir lättare att skala upp applikationerna vid behov.

En av de större riskerna kan vara att man som inköpare inte stämt av att ens egna krav och behov i förhållande till molntjänsten faktiskt beskrivs i avtalet. Leverantören kommer enbart att göra vad som framgår av avtalet och i vissa fall tillåts leverantören till och med ändra i villkoren för tjänsten under avtalstiden. Riskerna minimeras avsevärt om ni förstår ert eget företags infrastruktur och **genomför en behovs- och riskanalys** innan upphandlingen genomförs och använder analysen under upphandlingen av tjänsten. Ni bör vidare inte tillåta att leverantören ensidigt får ändra i tjänstens funktionalitet under avtalstiden.

Ni behöver vidare vara medvetna om vilka regelverk som ert data omfattas av, såsom den kommande dataskyddsförordningen (mer om detta senare) och vad det, ur ett dataskydds-perspektiv, innebär att anlita en extern part. Ni behöver exempelvis förstå vilken data som kan komma att samlas in av leverantören och var den kommer att finnas samt vilken säkerhetsnivå leverantören erbjuder. I de fall er data behöver överföras utanför EU kan detta vara en försvårande omständighet i riskanalysen.


“ ANSVAR KAN ALDRIG OUTSOURCAS ”
safespring

Vad är viktigast att tänka på när man väljer en molnleverantör?

Molntjänster brukar delas in i följande nivåer; **infrastruktur**, **plattform** och **mjukvara** som tjänst. Infrastrukturmolntjänster ersätter det traditionella datacentret och skapar därför en plattform för de egenutvecklade tjänsterna. Det finns inget som hindrar att man använder olika molnleverantörer för de olika nivåerna. Snarare kan det vara en fördel. Genom att analysera behoven kan en kombination av tjänster från olika nivåer och leverantörer ge den bästa totallösningen.
Ett möjligt utfall efter en analys kan vara att lägga de känsligare systemen i sin infrastrukturmolntjänst och samtidigt köpa andra tjänster som mjukvarutjänst från en annan leverantör.

Ur ett **tekniskt perspektiv** är det också viktigt att värdera vilka olika inlåsningsmekanismer man eventuellt drabbas av. Framförallt de stora publika molnleverantörerna har ett flertal så kallade microservices som är enkla och bekväma att ta i bruk. Tillsammans med proprietära lösningar i tjänsterna finns det dock en stor risk för att man som användare får det extremt svårt att flytta ut ur tjänsten. En exitstrategi är därför viktig att värdera redan innan man tar tjänsten i bruk.

En annan viktig aspekt är i vilken utsträckning man behöver kunna anpassa tjänsten efter sina behov, till exempel integrationer. Generellt kan man säga att ju större publik molnleverantör man väljer, desto mindre grad av anpassning erbjuder de.

Man måste också titta på den lagstiftning som leverantören lyder under. Detta gäller särskilt för internationella publika molnleverantörer som är verksamma i flera olika länder.
Om tjänsten innebär att molnleverantören behandlar personuppgifter måste parterna ingå ett databehandlaravtal med hänvisning till gällande personuppgiftslagstiftning. Generellt gäller det att ta hänsyn till vilken lagstiftning som påverkar ens valmöjligheter. Det kan vara fler regelverk utöver PUL och GDPR.

>> 5

Så hur bör man tänka runt backup av sin infrastruktur? I den klassificering av data man gör i sin kartläggning kommer olika data ha olika krav på backup. Genom en analys av den information man har i sina system kan en differentierad lösning sättas upp som är kostnadseffektiv och anpassad för organisationen. Till exempel är det är helt olika backupkrav på bilderna från er senaste kickoff jämfört med ert kundregister. Ändå är det inte helt ovanligt att samma regler sätts för all data i en traditionell backuplösning.

För **bästa resultat** ska ni göra en riktig design för molndriften, likt den nuvarande design ni förhoppningsvis har till ert eget datacenter för tillfället. Molnet kan användas på flera olika sätt, det viktiga är att ni drar nytta av tjänsterna istället för att fundera på hur de är implementerade.

6

Ska vi använda oss av en eller flera molnleverantörer?

Oftast brukar det bli så att IT-chefen tittar på verksamhetens centrala **behov** och utvärderar utifrån ett helhetsperspektiv. Ute i verksamheten är de ansvariga många gånger mer fokuserade på att hitta en leverantör som kan lösa en specifik utmaning. Här kan det ibland saknas samsyn i vad som bör väljas.

Ni kommer troligtvis inte att hitta en molnleverantör som tillgodoser alla dessa delar till hundra procent. Istället handlar det ofta om hur snabbt ni kan få komma igång, detta genom att ni designar era egna lösningar och hittar en leverantör med stor flexibilitet. Ett tips är att börja småskaligt, med ett system i taget. Olika leverantörer är bra för olika tjänster.

“MOLNTJÄNSTER FRIGÖR TID. LÄGG DEN TIDEN PÅ ATT UTVECKLA DITT FÖRETAG I RÄTT RIKTNING OCH I DE FRÅGOR NI FAKTISKT BRINNER FÖR”

safespring

7 Vilka krav bör man ställa på en molnleverantör vad gäller outsourcing av infrastrukturtjänster?

Det är främst tre perspektiv man ska fundera kring; det **juridiska**, det **säkerhetsmässiga** och det **kommersiella**. Juridiken berör compliance, alltså vad som ligger i linje med gällande lagar, samt databehandling. Säkerheten berör det rent operationella. Ett tips här är att välja en lokal leverantör där ni själva kan undersöka datahallarna. Det kommersiella berör flexibilitet i kostnader så att ni kan optimera tjänsterna.

Först och främst bör ni säkerställa att avtalet med molntjänstleverantören ger er rätt att använda tjänsten på det sätt ni önskar och att tjänsten har den efterfrågade funktionaliteten, samt att det finns tillräckliga regleringar avseende tillgänglighet, support och servicenivåer. Det är även viktigt att man som kund vet vilken flexibilitet tjänsten har eftersom upp- och nedskalning av volymer ofta är ett viktigt skäl till varför man har valt en molntjänst.

Ur ett juridiskt perspektiv bör ni, oavsett om ni köper in tjänsten före eller efter dataskydds-förordningen (GDPR) träder i kraft den 25 maj 2018, ställa krav på att molntjänstleverantören har vidtagit åtgärder för att kunna leverera en tjänst som är förenlig med GDPR. Som inköpare kommer ni högst sannolikt att vara ansvariga för de personuppgifter som molntjänstleverantören behandlar för er räkning. Till exempel får ni då endast anlita en leverantör (under GDPR kallat **”personuppgiftsbiträde”**) som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i GDPR. Vilka faktiska åtgärder detta innebär i det enskilda fallet beror i stor utsträckning på vilken typ av personuppgifter som behandlas, hur behandlingen går till och hur många individer som är registrerade.

GDPR ställer även krav på att avtal med personuppgiftsbiträden ska innehålla vissa särskilda skrivningar, vilket ni bör ställa krav på att avtalet med **molntjänstleverantören** gör. Att inte uppfylla kraven i GDPR är inte endast en kommersiell risk utan kan även medföra dryga böter och skadestånd.

>> 7

Vidare finns en säkerhetsaspekt avseende det rent operationella. Vissa kunder behöver kunna genomföra inspektioner och verifiera efterlevnad av ingånget avtal hos leverantören, medan andra ställer krav på kryptering av data.

Det finns alltså många frågor att ställa till leverantören innan beslut tas. Vilken service-nivå levereras? Finns det support och hur kan ni kontakta serviceleverantören? Är det bara via mail eller kan man ringa? Gäller det dagtid eller dygnet runt? Är det viktigt för er att få support på lokalt språk? Hur ser tillgängligheten ut och vad händer vid överträdelser? För er som användaren är det viktigt att förstå vilken service-level (SLA) man kan förvänta sig och vilka konsekvenser det skulle bli om leverantören inte lever upp till avtalad servicenivå.

8 Vilka lagar måste vi hålla koll på när det gäller datahanteringen?

Det beror på vilken typ av verksamhet ni ägnar er åt. Förutom **PUL** och den kommande **GDPR**-lagen så finns det ju en mängd fler lagar och krav baserat på verksamhetsområde. Till dessa hör lagar som Patientdatalagen, Arkivlagen med flera.

Om molntjänstleverantören kommer att behandla personuppgifter för er räkning är det idag personuppgiftslagen (1998:204) (PUL) som är aktuell, men från och med den 25 maj 2018 är det dataskyddsförordningen (GDPR) som gäller. Såväl PUL som GDPR kompletteras dock av andra lagar som kan bli tillämpliga i det enskilda fallet. Utöver detta kan andra lagar också bli tillämpliga beroende på vilken typ av molntjänst som införskaffas och vad den ska användas till, såsom exempelvis patientdatalagen (2008:355), arkivlagen (1990:782) eller tulldatalagen (2001:185).

>> 8

Det största problemet många företag har är att det inte gjort någon ordentlig inventering innan, till exempel vilken skyddsvärd data man faktiskt har i sina system. Det är viktigt att göra den kartläggningen eftersom ansvar aldrig kan outsourcas.

9

Kan en backup i molnet bättre skydda oss från virus?

Virus och **malware** kan kryptera allt på din dator, även servrar och gemensamma enheter, fysiska liksom virtuella. Denna typ av kryptovirus, också kallat **ransomware**, är en av många anledningar till varför man ska ha en bra backupplan för sina filer. Risken här ligger också i att det kan ta tid att upptäcka att ens nätverk har smittats. Då kan flera dagars backup redan vara påverkad.

Viruset använder de vanliga filserverprotokollen för att förflytta sig, så en extern backuplösning är det bästa sättet att skydda sig. Se till att välja en backupleverantör med bra **retentiontid** och stor **kapacitet**. Då tas backup vid flera tillfällen och sparas, vilket gör att ni kan gå tillbaka flera dagar för att återfå filerna från tiden innan de blev infekterade.

“HUR LÄNGE TÅL ER VERKSAMHET ATT STÅ STILL I VÄNTAN PÅ ÅTERSTÄLLNING?”

safespring

Vilka säkerhetsmetoder ska vi leta efter hos molnbackupleverantören?

Om man ska kunna skydda sin data samtidigt som kopior lagras i molnet måste man göra en design baserad på en medveten **misstro** leverantören eller nätoperatörerna emellan. Data ska alltså aldrig överföras i klartext till molnet, utan krypteras före eller under tiden den sänds och sedan lagras på självkrypterande media. Det är dels för att datan ska kunna vara hemlig för molnleverantören och för att företaget som outsourcat datan ska känna sig trygga med det. Det är även för att skydda datan från **hackare** utifrån eller vid byte av hårddiskar.

Om det rör sig om extremt känslig data kanske man till och med ska kryptera den en extra gång, redan innan den förs över till tjänsten, men då sitter enbart ett fåtal personer på företaget på nyckeln till krypteringen. Molnleverantören kan alltså inte hjälpa er om nyckeln tappas bort, men ni har hundraprocentig kontroll över vem som kan läsa datan.

Vem är admin och äger datan efter en outsourcing?

Det är ni som kund som är ägare av den data som laddas upp och bearbetas i molnet och det rekommenderas att detta tydligt framgår av avtalet. När avtal för molnleverantör skrivs kommer ni överens om sådana här saker och **reglerar** detta själva. Även om ni äger filerna är det viktigt att förstå vilka lagar gällande utlämnande av data som molnleverantören lyder under. En svensk molnleverantör lyder under svenska lagar.

Ni ska vidare kunna kontrollera datan på administratörsnivå. Molntjänstleverantören ska endast ha rätt att använda data för att fullgöra sina förpliktelser under avtalet, det vill säga att leverera tjänsten. Tydlighet rörande rätten till datan är A och O.

12 Hur kommer en migration av infrastrukturtjänsterna att påverka IT-chefens roll på företaget?

Dagens **digitalisering** leder till att IT-avdelningen ofta ska leverera en högre grad av IT-stöd till organisationen. Samtidigt får de sällan mer resurser till detta.

Server-, lagrings- och hårdvara är idag ofta standardiserad hyllvara. Att slippa planläggning för utbyggnad, drift och underhåll av detta, som isolerat i sig levererar ett begränsat mervärde till företaget, frigör tid och resurser för att göra mer verksamhetsnära IT.

Det blir alltså mindre jobb med att assistera hårdvarorna och man får en månadskostnad där man enklare kan se hur det utvecklar sig under tiden. Det leder i sin tur till att mer tid kan användas till att **automatisera** IT-stödet för att jobba effektivare och modernare. IT-chefens roll blir att leda det strategiska arbetet.

13 Vad händer med vår data om molnleverantören går i konkurs eller drabbas av någon naturkatastrof?

Om er molnleverantör skulle gå i konkurs och försvinna från marknaden så träder en **konkursförvaltare** in och övertar driften. Därför kan det vara viktigt att man har avtalat om rätt att häva avtalet. Vid avtalets upphörande börjar ni exekvera er **exitstrategi**, som måste vara på plats.

Vad gäller katastrofer, till exempel om datahallarna helt plötsligt skulle brinna ned, så får man redan i sin inventering fundera på hur kritiskt detta är. Se till att välja en molnleverantör som har flera datahallar och uppge önskemål på att er backup ska finnas i flera av dessa. Om dina backuper är **geografiskt åtskilda** från primärdatan är det osannolikt att samma brand eller katastrof drabbar båda samtidigt.

14 Hur lång tid kan det skilja i att återfå sin data beroende på backupleverantör?

Det varierar rätt stort och baseras bland annat på mängden datafiler. Det handlar också om vad ni har kommit fram till i ert avtal med leverantören. Generellt kan man säga att det kan skilja allt-ifrån några dagar till flera månader att återfå sina filer beroende på leverantör, storlek, bandbredd och vad ni kommit överens om. Frågan ni bör ställa er är hur länge er verksamhet tål att stå still i väntan på återställning.

15 Hur mäter vi förväntad framgång när det gäller outsourcing av infrastrukturtjänster?

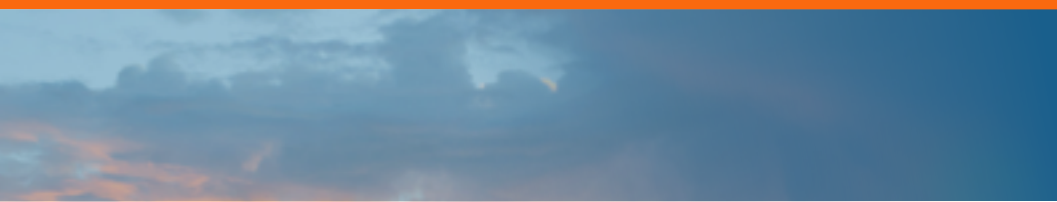
Tid mäts i timmar och pengar mäts i kronor. Men vad mäter man nytta i? För att mäta de ekonomiska utfallen är det viktigt att man mäter hela livscykelkostnaden för en egen investering i hårdvara. Sedan kan man jämföra det med att köpa resurser som tjänst. Det räcker alltså inte med att jämföra med inköpskostnaden för hårdvara. Man måste även inkludera de interna kostnaderna för drift, konfiguration, patchning och övervakning samt support och underhålls-avtal under avskrivningsperioden. För att få en riktigt jämförbar siffra bör man även inkludera hyra för den egna datahallen samt strömförbrukning och kyla.

Det rekommenderas att man först gör en intern inventering av den totala kostnaden för en tjänst som man själv producerar samt uppskattar vad en förbättring i flexibilitet med mera som erbjuds i en molntjänst skulle kunna innebära. Det är sedan viktigt att man efter mätning sätter upp de egna relevanta mätetal man kommit fram till, för att sedan kunna visa på vad införandet av infra-strukturtjänster faktiskt har bidragit med.

Om ni från början gjort rätt med er molndesign kommer det bli oerhört lätt att mäta exempel-vis time-to-market. Att göra nyetableringar kommer även bli enklare om ni tänkt rätt vad gäller verktyg. Istället för att ni måste bygga en ny serverpark, vilket kan ta månader, så är ni bara ett knapptryck ifrån att starta igång en ny sajt. Allt detta är en del av den kravbild ni får framföra till er utvalda molnleverantör.

Checklista på frågor att ställa till leverantören

- Exakt vad är det leverantören erbjuder?
- Vad kostar det att outsourca sin backup?
- Vilka betalningsmodeller erbjuds?
- Vilken flexibilitet finns det hos leverantören för att passa våra behov?
- Hur lång tid tar det att skapa en backup?
- Vilken storlek på backup kan leverantören tillhandahålla?
- Hur snabb är uppkopplingen?
- Hur ser deras SLA ut?
- Har de en lokal support som talar svenska?
- Hur får jag tag i dem?
- Vilken säkerhet har leverantören, både vad gäller virtuell och fysisk säkerhet?
- Hur lång tid tar det att återskapa min data vid en intern krasch?
- Vilka återställnings- och kontinuitetsalternativ finns det om katastrofen slår till?
- Hur lätt kan vi flytta ut ur tjänsten om vi skulle önska det i framtiden



safespring

Ordlista för infrastrukturtjänster i molnet:

Infrastrukturtjänst - även kallat IaaS eller Infrastructure-as-a-Service är en virtualiserad miljö som omfattar serverkapacitet, nätverk, lagring och säkerhet som tillsammans ger en kostnadseffektiv och skalbar miljö för ett privat eller publikt moln. Ovanpå det så installerar man sitt operativsystem och applikationer. Det är kundens ansvar att drifta och övervaka dessa.

GDPR – Står för *General Data Protection Regulation* och är ett nytt EU-direktiv som träder i kraft i maj 2018. Lagen kommer att gälla alla företag som på något sätt samlar in, lagrar eller processar personuppgifter.

Safeharbour – Detta var en överenskommelse som framtogs 1995 mellan EU och USA om personuppgiftsskydd. Den blev ogiltigförklarad 2015.

SLR – Står för *Service-level agreement*, eller serviceavtal. Det är det avtal som skrivs mellan kund och leverantör för att den överenskomna nivån för service och support ska kunna garanteras.

RTO – Står för *Recovery Time Objective*, vilket handlar om hur snabbt ni kan vara tillbaka på banan igen efter en IT-krasch.

RPO – Står för *Recovery Point Objective*, vilket handlar om hur ofta ni vill att en backup ska tas, alltså hur många dagars arbete ni kan stå ut med att förlora.

Ransomware – Samlingsnamn på skadliga programvaror som tar dina filer som gisslan för att sedan avkräva dig en summa pengar om du vill ha tillbaka filerna. Typiskt för dessa program är att de krypterar dina filer och kostnaden du avtvingas ligger i att du måste låsa upp allt igen.

DPO – Står för *Data Protection Officer* och är titeln på den person på företaget som är ansvarig för att interna bestämmelser om personuppgiftshantering följs.

3-2-1-regeln – En hållpunkt som ofta omnämns när man pratar om backup. Regeln innebär att den bästa backupen består av tre kopior, varav två finns lokalt och en geografiskt åtskild från de andra. Den regeln må vara bra för vilande data, men för exempelvis transaktions- data är det inte tillräckligt utan kompletterande krav för RTO och RPO.

safespring

Om Safespring

Safespring levererar lokalt producerade molntjänster designade för framtidens behov och applikationer. Våra tjänster lever upp till högt ställda krav på säkerhet, liksom lokala lagar och regler – idag och i framtiden. Våra kunder skapar sig konkurrensfördelar genom flexibilitet utan tekniska begränsningar – och till en avsevärt lägre kostnad än tidigare.

Med Safesprings molnbaserade backuptjänst (BaaS) behöver du inte investera i egen hård- eller mjukvara. Tjänsten konsumeras över internet och du betalar bara för den mängd data som sparas i tjänsten.

Vill du veta mer om Safespring, kontakta Fredric Wallsten, VD.
Tel: (+46) 0766 - 29 25 02

Registrera dig för en gratis demo redan idag!

IBM Business Partner

www.safespring.com | info@safespring.com

safespring