Kontinuitetsplanering – en introduktion

KRISBEREDSKAPS
MYNDIGHETEN

Titel: Kontinuitetsplanering – en introduktion.
Utgiven av Krisberedskapsmyndigheten (KBM)
Text: Andreas Malm
Omslagsfoto: Pressens Bild
Illustratör: Kari Modén
Produktion: Jupiter Reklam AB
KBM:s Dnr: 1227/2006
Skriften kan laddas ner från Krisberedskapsmyndighetens hemsida
www.krisberedskapsmyndigheten.se

"I samhället är helheten, precis som kedjan, inte starkare än den svagaste länken, det vill säga det enskilda företaget."

Konsten att överleva förlusten av operativ förmåga

I dagens komplexa infrastruktur och samhällskonstruktion kan få företag verka utan väsentliga leverantörer och samhällsfunktioner. Om ett företag inte längre kan leverera sina tjänster eller produkter drabbas andra företag som i sin tur påverkar ännu fler. Ett företags arbete med att säkra sin leveransförmåga är därför av vikt inte bara av affärsmässiga skäl, utan även för samhället i stort.

Tre principer är centrala i samhällets krishanteringssystem: **ansvarsprincipen, likhetsprincipen** och **närhetsprincipen**.[1] **Ansvarsprincipen** gör gällande att den som har ansvar för en verksamhet under normala förhållanden också ska ha ansvaret under krissituationer. **Likhetsprincipen** innebär att en verksamhets lokalisering och organisation så långt det är möjligt ska vara densamma såväl under fredstida förhållanden som under kris eller krig. **Närhetsprincipen** innebär att en kris ska hanteras där den inträffar och av dem som är närmast berörda och ansvariga.

> Det är viktigt att företag planerar för att stärka sin förmåga till fortsatt verksamhet vid alla typer av störningar eller händelser. Likaså att kritiska processer kan återstartas inom en för verksamheten tolerabel tidsrymd.

Under senare år har kontinuitetsplanering vuxit fram som en metod för att säkra olika verksamheters leveransförmåga. Metoden skapar en robusthet som innebär att företag bättre kan överleva förluster av delar eller hela sin operationella förmåga. Med detta menas att företaget minskar sin sårbarhet och ökar sin motståndskraft mot olika händelser som kan påverka dess kritiska verksamhet. Med ett utvecklat program för kontinuitetsplanering klarar

[1] Krisberedskapsmyndigheten (2006), Att planera inför en pandemi – en vägledning för verksamhetsansvariga, 2006, KBM:s dnr: 0216/2006

verksamheten av att under ett avbrott leverera de tjänster och produkter som är viktigast för företaget och dess kunder. Det har samtidigt utvecklade rutiner för att snabbt kunna återgå till normal verksamhet efter ett avbrott.

Kontinuitetsplanering kan därför vara ett bra komplement till befintliga verktyg och metoder som syftar till att öka såväl ett företags som samhällets samlade krishanteringsförmåga.

Genom kontinuitetsplanering stärks företagen, det vill säga länkarna, och således även helheten. Indirekt kan därför kontinuitetsplanering bidra till det samhälleliga skyddet av såväl människor som egendom och miljö.

Kontinuitetsplanering kan tillämpas inom olika organisationer, privata som offentliga.[2] Det finns en mängd olika verktyg och modeller tillgängliga för att genomföra kontinuitetsplanering. Valet bör göras mot bakgrund av tillgängliga resurser och typen av risk i varje enskilt fall. Denna introduktion beskriver kontinuitetsplanering och visar hur företag kan dra nytta av metoden.

KONTINUITETSPLANERING =
en metod för att säkerställa företagets leveransförmåga genom att planera för fortsatt verksamhet vid förlust av operativ förmåga. Det vill säga att trots avbrott kunna leverera de tjänster och produkter som är viktigast för företaget och dess kunder.

[2] Det saknas en heltäckande internationell standard. Följaktligen finns ingen enhetlig terminologi eller svensk översättning av de olika begreppen. Gemensamt för de olika modellerna är dock helhetssynen på kontinuitetsplanering som process med fokus på affärskritiska verksamheter. Utvecklingen av en internationell standard inom kontinuitetsplanering pågår. Arbetet leds av den tekniska kommittén ISO/TC223.

Kontinuitetsplanering

Trots att terroristangrepp och naturkatastrofer får de stora rubrikerna är nästan 90 procent av alla kriser i ett företag orsakade av händelser som inte får nyhetsrubriker.[3] Många gånger är dessa kriser orsakade av händelser som gjort det svårt att bedriva affärskritiska verksamheter, såsom att leverera tjänster och produkter till kunder. Genom att öka förutsättningarna för kontinuitet i dessa verksamheter, oavsett vilka händelser som inträffar, har kontinuitetsplanering väckt ett stort intresse bland företag runt om i världen.

Under de senaste åren har metoden utvecklats från att ha ett IT-fokus till att ha ett verksamhetsövergripande perspektiv.[4] Det innebär att kunskapen om vad som är affärskritiskt inte begränsas till att enbart omfatta företags IT-processer och IT-system. Vad som kan betecknas som affärskritiskt är i stället alla de processer som är viktiga för att företaget ska kunna uppnå sina verksamhetsmål. Dessa processer kan i sin tur kräva stödprocesser, aktiviteter och resurser. De sistnämnda kan vara personal, system, funktioner och tjänster som finns i den egna verksamheten eller som levereras av ett externt företag.

Ett år efter attackerna i London den 7 juli 2005 gjordes en undersökning av 161 företag. Den visade att arbetet med kontinuitetsplanering framgångsrikt bidragit till att verksamheter kunnat upprätthållas under och efter krisen. Nästan hälften av de intervjuade företagen aktiverade sina kontinuitetsplaner och 90 procent av dessa var nöjda med effektiviteten i planerna.[5]

Kontinuitetsplanering hjälper verksamheter att optimera sina investeringar i den affärskritiska säkerheten och robustheten. Genom att systematiskt analysera de aktiviteter och resurser som är viktiga för de affärskritiska processerna kan

[3] Så kallade "quiet catastrophes", BCI, Business Continuity Institute (2005), Good Practice Guidelines – A framework for Business Continuity Management, www.thebci.org.

[4] Finansinspektionen (2004), Från elavbrott till 11 september – kriser, erfarenheter, lärdomar. www.finansinspektionen.se

[5] Både stora och små företag, där knappt 25 procent av dessa hörde hemma i den finansiella sektorn, 16 procent i den offentliga sektorn och 7 procent i energi- och telekomsektorn. ICM and Continuity Central (2006), July 7th 2005: Looking back for the future, www.continuitycentral.com

brister i säkerheten och redundansen upptäckas. Men man kan även avslöja en onödigt hög redundans hos exempelvis system och personal.[6] Fördelningen av resurser för säkerhet och redundans kan därmed optimeras mot bakgrund av vilka processer, aktiviteter och resurser som är särskilt betydelsefulla för företaget.

Kontinuitetslösningar och kontinuitetsplaner kan utgöra viktiga element i företagets strategi för att hantera risker.

Kontinuitetsplanering och riskhantering

Riskhantering är ett affärsbyggande verktyg som handlar om att hantera osäkerheter genom att systematiskt värdera och behandla de risker som är oundvikliga för att nå ett eller flera mål. Alla typer av risker kan värderas och behandlas utifrån acceptanskriterier som beskriver hur stora risker ett företag är villigt att ta. Dessa kriterier fastslås i regel utifrån dess aktuella marknad. Även den juridiska, sociala, politiska och kulturella miljön påverkar riskbenägenheten.

Inom kontinuitetsplanering skapar riskvärdering en fördjupad förståelse för risker kopplade till de affärskritiska processerna. Det gör den till ett verktyg och en viktig komponent. Syftet med riskvärderingen är att identifiera, analysera och utvärdera de risker ett företag möter i anslutning till sina affärskritiska processer. Riskerna kan vara av intern eller extern karaktär och utvärderas i regel utifrån en händelses sannolikhet och konsekvens. Mot bakgrund av företagets acceptanskriterier (exempelvis toleransen mot möjliga störningar) utvecklas en handlingsplan för hanteringen av dessa risker. Normalt prioriteras de affärskritiska processer som är utsatta för störst risk och har lägst tolerans för störningar.

Här skiljer sig kontinuitetsplaneringens riskvärdering från den övergripande. Risker som är låga eller inte kopplade till affärskritiska aktiviteter kommer i regel inte att hanteras.

[6] Mindre betydelsefulla resurser och system kan ha en "onödigt" hög redundans (exempelvis att ett stödsystem inte behöver vara dubblerat).

Riskhanteringen i stort kan dock av andra skäl, exempelvis ekonomiska, välja att prioritera och hantera även dessa risker. Erfarenheter visar att ett effektivt arbete med kontinuitetsplanering sänker företagets riskprofil, vilket kan resultera i lägre försäkringspremier.

Kontinuitetsplanering skyddar marknadsandelar

Branden i Albuquerque visar hur bristande förmåga att värdera och hantera händelser kan få allvarliga konsekvenser för ett företag. Philips Electronics komponentfabrik för radiofrekvenschips i Albuquerque, New Mexico, utgjorde en strategisk leverantör till både Nokia och Ericsson. Fabriken drabbades av en mindre brand år 2000. Inom loppet av ett par dagar informerade Philips sina kunder om branden, som inledningsvis inte antogs ha några större effekter på den fortsatta produktionen.

Trots den begränsade informationen från Philips valde Nokia att aktivera sin krishanteringsgrupp för att hantera händelsen. Högsta ledningen involverades och beslut togs om omkonstruktion av chipen för att kunna använda en annan leverantör, om detta blev nödvändigt. Nokia fattade även beslut om produktionsökningar i befintliga anläggningar och genomförde kraftfulla förhandlingar med Philips för att säkra leveranserna av de viktiga komponenterna från andra fabriker – i händelse av att produktionsbortfallet i Albuquerque skulle bli långvarigt.

Hos Ericsson uppfattades inledningsvis inte branden som någon potentiellt större kris och det tog veckor innan företaget förstod de möjliga konsekvenserna. Bristande kommunikation ledde till att Ericsson agerade först efter att Nokia bundit upp Philips resurser. Ericsson hade ett kritiskt beroende till Philips komponenter, men ingen "plan B" för hur företaget skulle agera om leveranserna plötsligt skulle upphöra, enligt marknadschefen hos Ericsson.

Branden orsakade ett totalt produktionsbortfall vid fabriken i Albuquerque under knappt sex månader. För Ericsson

avstannade produktionen av företagets mobiltelefoner i flera månader. De ekonomiska konsekvenserna blev en förlust på motsvarande fyra miljarder kronor. Nokias hantering, däremot, ledde till att företaget kunde återgå till full produktion utan större avbrott och sammantaget kunde Nokia öka sin marknadsandel under denna period.[7]

Krishantering påverkar varumärke och börsvärde

Branden i Albuquerque utgör ett av många exempel som visar på att ett företags varumärke och marknadsvärde påverkas av hur väl en kris hanteras.[8] Bristande krishantering kan innebära ett avsevärt försämrat börsvärde.

I ett initialt skede har alla kriser en negativ inverkan på börsvärdet. Efter en skarp nedgång av börsvärdet sker ofta en återhämtning. På längre sikt är det dock stor variation mellan olika företag och deras respektive återhämtningsförmåga. Företag med en effektiv krishantering kan redan efter 50 handelsdagar uppvisa ett ökat börsvärde. Företag med ineffektiv krishantering kan däremot uppvisa ett försämrat börsvärde motsvarande omkring 15 procent ända upp till ett år efter att krisen inträffat.[9] När företag väl hamnat i en kris kan det behöva tre år för att återvinna marknadens förtroende.[10] Mot bakgrund av tillgänglig forskning står det idag relativt klart att en förmåga till effektiv krishantering är av mycket stor vikt för alla företag.

Effektiv krishantering
= ökat börsvärde

Ineffektiv krishantering
= sänkt börsvärde

[7] Utdrag ur Yossi och Sheffi (2005), The Resilient Enterprise – Overcoming vulnerability for competitive advantage, The MIT Press, Cambridge, Massachusetts, USA

[8] Rory F. Knight & Deborah J. Pretty (2005), The Impact of Catastrophes on Shareholder Value, Oxford Metrica Ltd

[9] ibid

[10] Burson-Marsteller, pressmeddelande, 23 augusti 2006. Baseras på intervjuer i 85 länder med direktörer, journalister och företrädare för myndigheter.

Kontinuitetsplanering och krishantering

Kontinuitetsplanering är en metod som kompletterar och underlättar krishanteringen om och när denna blir nödvändig. Metoden ersätter dock inte krishantering. Alla företag kan uppleva kriser utan att deras affärskritiska processer blir störda. Likaledes kan de uppleva störningar i sina affärskritiska processer, som hanteras genom kontinuitetslösningar och kontinuitetsplaner, utan att detta i sig innebär en kris för verksamheten.

Kontinuitetsplanering och skyddet av kritisk infrastruktur

I augusti 2003 drabbades delar av nordöstra USA och Kanada av ett omfattande elavbrott. Det sammankopplade eldistributionssystemet i nordöstra USA är komplext, dynamiskt och svårt att överblicka. I detta fall ledde bristande övervakning i kombination med ett par simultana fel till kaskadeffekter. Elförsörjningen i hela regioner slogs ut. På grund av elbortfallet drabbades även andra infrastrukturer av händelsen.[11] Transportsektorn påverkades genom att signalsystem slutade fungera, något som fick konsekvenser för exempelvis tunnelbanesystemet i New York. Vattenförsörjningen i Cleveland och Detroit påverkades då reningssystemen upphörde att fungera och delar av tillverkningsindustrin i Ohio och Michigan fick stänga. Totalt berördes så många som 50 miljoner människor av elavbrottet som inträffade vid 16-tiden, det vill säga efter aktiemarknadernas stängning.

> Elavbrottets direkta kostnad: 4-10 miljarder. Kanadas BNP sjönk med 0,7 procent under augusti månad.

Under krisen visade det sig att företag som hade förberett sig för stora elavbrott i sin kontinuitetsplanering hade svårt att upprätthålla sin verksamhet trots gjorda investeringar i reservaggregat och upprättade planer. Orsaken var att deras underleverantörer och kunder i sin tur inte kunde verka på grund av bristfälliga förberedelser. Elavbrottet visade att komplexa och kritiska beroendeförhållanden i

[11] R. Zimmerman, C. E. Restrepo (2006), The next step: quantifying infrastructure interdependencies to improve security, International Journal of Critical Infrastructures 2006 – Vol 2, No. 2/3 sid 215-230

dagens samhälle skapar ett behov av riktlinjer för kontinuitetsplanering inom en sektor eller ett visst geografiskt område.[12] Allt fler länder utvecklar följaktligen riktlinjer för kontinuitetsplanering inom finansområdet, telekommunikation och för annan samhällsviktig verksamhet.

Kontinuitetsplanering som skydd för det affärskritiska processerna

En systematisk kontinuitetsplanering utvecklar strategier, lösningar och planer som säkerställer kontinuitet i de affärskritiska processerna. Därigenom uppnår verksamheten ett antal fördelar:

- **Trygghet** – ett systematiskt tillvägagångssätt minskar risken för att missa viktiga detaljer
- **Effektivitet** – investeringar i säkerhet och kontinuitet optimeras i förhållande till hur viktig en process är för verksamheten i stort
- **Transparens** – ledningen i ett företag tvingas fatta beslut och kommunicera organisationens riskaptit, det vill säga viljan att ta risker
- **Ansvar** – genom ett strukturerat arbete tydliggörs ansvaret för kritiska delar av verksamheten.

[12] Finansinspektionen (2004), Från elavbrott till 11 september – kriser, erfarenheter, lärdomar, www.finansinspektionen.se

Att kontinuitetsplanera

Kontinuitetsplanering skapar en grundläggande medvetenhet om företagets affärskritiska processer och dess tolerans mot störningar, liksom vilka risker och sårbarheter verksamheten är exponerad mot. Utifrån denna medvetenhet skapas och anpassas kontinuitetslösningar och planer för att säkerställa kontinuiteten i de affärskritiska processerna. I takt med att omvärlden förändras och att företaget utvecklas måste kontinuitetslösningar och planer anpassas och kontinuerligt verifieras. Det är därför vanligt att verksamheterna skapar ett program för kontinuitetsplanering som en del av företagets övergripande riskhantering. För att implementera och driva ett program för kontinuitetsplanering finns det ett antal framgångsfaktorer.[13]

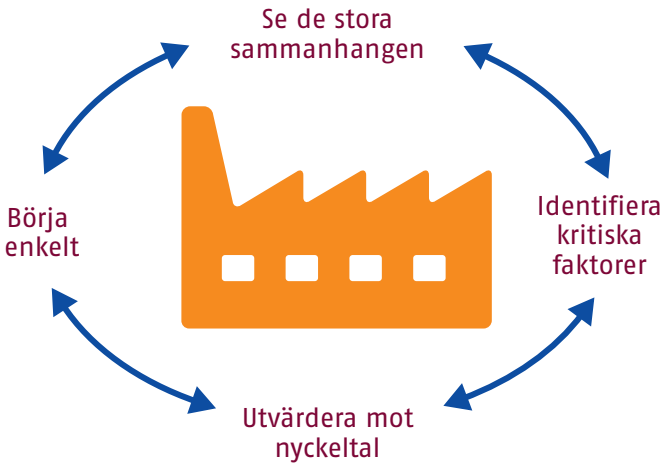
Framgångsfaktorer

Helhetsperspektiv på den affärskritiska verksamheten

Kontinuitetsplaneringen bör som ett minimum omfatta verksamhetens samtliga affärskritiska processer och aktiviteter. Den bör kännetecknas av ett systemperspektiv, där företaget betraktas som en del av ett större sammanhang. Det är nämligen viktigt att förstå hur företagets beroenden av andra kan påverka den egna förmågan att leverera tjänster och produkter. Det är också av vikt att förstå hur ett avbrott i den egna verksamheten kan påverka andra företag och funktioner i samhället.

Se den egna verksamheten i ett större sammanhang!

[13] Flertalet av dessa framgångsfaktorer har identifierats i samband med produktionen av Goda Exempel rörande kontinuitetsplanering. Dessa Goda Exempel finns tillgängliga på Krisberedskapsmyndighetens webbplats, www.krisberedskapsmyndigheten.se



Ledningens engagemang och målstyrning

Kontinuitetsplaneringen är en del av en effektiv verksamhetsstyrning som kräver ledningens engagemang. Ledningen kan visa detta genom att exempelvis etablera interna nyckeltal kopplade till framsteg inom kontinuitetsplaneringsarbetet. Genom att kontinuerligt definiera och utvärdera olika utvärderingsmått skapas förutsättningar för spårbarhet och ständiga förbättringar i arbetet. Här kan verktyg såsom benchmarking[14] mellan företagets olika avdelningar utgöra en effektiv mekanism för att stimulera arbetet med kontinuitetsplanering.

Utvärdera genom interna nyckeltal!

Kontinuitetsplanering som en del av företagskulturen

Arbetet med kontinuitetsplanering syftar inte till att åstadkomma ett dokument som för ledningen redovisar risker och sårbarheter. En effektiv kontinuitetsplanering är en process som involverar och engagerar hela företaget i arbetet med att skapa kunskap om vilka aktiviteter och

[14] Benchmarking innebär att jämföra förhållanden hos olika enheter mot en förutbestämd måttstock.

resurser som är kritiska för verksamheten. Den bör ge förutsättningar att förstå osäkerheter i framtiden och hur olika avbrott påverkar såväl den egna verksamheten som externa intressenter. Detta för att bättre kunna planera för att både förebygga och hantera framtida avbrott.

Identifiera kritiska faktorer!

Enkelhet

Erfarenheter visar att enkelhet är viktigt vid utformandet av ett program för kontinuitetsplanering. Det är därför viktigt att inledningsvis inte sätta ribban för högt. Bättre då att höja kraven ju skickligare man blir. Här kan avgränsningar i arbetet till en början göras. Kontinuitetsplanering på en liten avdelning eller för en begränsad affärskritisk process kan exempelvis utgöra ett pilotprojekt. Kontinuitetsplaneringsarbetet är ett långsiktigt arbete som ständigt kan förbättras, men som riskerar att stanna av eller helt utebli om individerna i företag inte klarar av att använda metoderna och verktygen.

Börja enkelt – öka omfång och djup efter hand!

Kontinuitetsplanerings-processens komponenter

En kontinuitetsplaneringsprocess innehåller ett antal distinkta komponenter. Dessa kan vara affärskonsekvens-analys, riskvärdering, kontinuitetsstrategi, kontinuitets-lösningar, kontinuitetsplaner, krishanteringsplaner, utbildning, övning och revision liksom kultur och upp-följning. Komponenterna går att finna i olika nationella standarder (som utgör ingångvärdet för utvecklingen av en internationell standard).[15]

Kontinuitetsplaneringsprocessen

[15] NFPA 1600, BS 25999-1 och HB 221:2004 tillsammans med bidrag från Japanese Industrial Standards Committee och Standards Institution of Israel, utgör grunden i framtagningen av en internationell standard på området. De komponenter som redovisas här återfinns i de flesta av dessa nationella bidrag/standards.

Affärskonsekvensanalys

Affärskonsekvensanalysen skapar kunskap om företagets affärskritiska processer, aktiviteter och resurser.

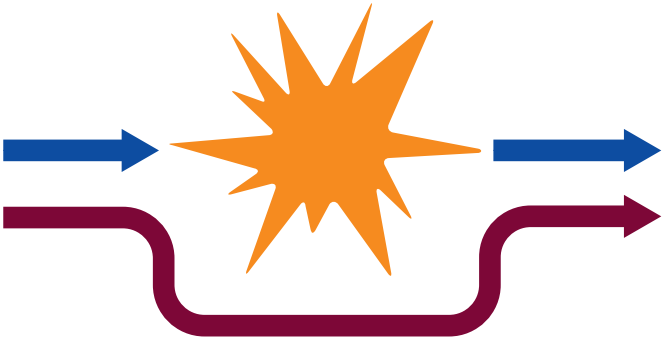
Att genomföra en affärskonsekvensanalys kan utgöra det första steget i en kontinuitetsplaneringsprocess. Analysen ger en fördjupad kunskap om de aktiviteter som olika avdelningar och enheter utför, för att stödja de affärskritiska processerna. Aktiviteterna utförs i regel med hjälp av resurser av olika slag – personal, system, utrustning och liknande.

Produktutveckling kan exempelvis vara en affärskritisk process för ett företag som levererar krockkuddar till bilar. En avdelning för utveckling av sensorer genomför en rad olika aktiviteter såsom design, simulering och konstruktion. För att utföra aktiviteten krocksimulering är företaget beroende av två nyckelpersoner och en så kallad Cray-dator med mycket hög kapacitet. Under vissa skeden är det särskilt betydelsefullt att dessa aktiviteter kan utföras utan större avbrott, för att inte produktutvecklingsprocessen ska påverkas. Ett avbrott i produktutvecklingsprocessen på grund av att krocksimuleringarna inte blir genomförda i tid kan innebära direkta ekonomiska konsekvenser för företaget. Om krockkuddarna inte kan levereras till kund i tid kan även företagets anseende påverkas. Med hjälp av en affärskonsekvensanalys kan företaget konstatera att under vissa skeden (worst-case) kan ett avbrott i krocksimuleringen enbart tolereras om det är kortare än åtta timmar.

Sådana kunskaper om maximalt tolerabel avbrottstid gör att företaget kan planera för säkerställd tillgänglighet hos aktiviteterna när de verkligen behövs.

Affärskonsekvensanalysen handlar om att systematiskt skapa kunskap om vad som är kritiskt för företaget. Analysen kan innefatta följande moment:

- Identifiera företagets affärskritiska processer. En affärskritisk process stödjer ett eller flera av de verksamhetsmål som finns i företaget.
- Identifiera de aktiviteter som stödjer processerna. Dessa aktiviteter levereras normalt av en enhet, avdelning eller funktion inom företaget.
- Definiera de krav företaget måste ställa avseende maximalt tolerabel avbrottstid för varje kritisk aktivitet. Hur lång tid kan leveransen av en sådan aktivitet ligga nere utan att detta skapar konsekvenser för företaget som inte kan anses som tolerabla?



Första steget är att definiera den maximalt tolerabla avbrottstiden. Företaget skapar därefter de reservvägar som krävs för att avbrottstiden aldrig ska bli längre än så.

Beroendeanalys

För att kunna utföra de kritiska aktiviteterna krävs resurser i form av exempelvis personal, system, utrustning eller leverantörer. Resurserna kan finnas internt i företaget eller köpas externt av en leverantör. En beroendeanalys kan ge en fördjupad kunskap om vilka resurser som är kritiska för verksamheten. I vårt exempel var de två nyckelpersonerna och Cray-datorn avgörande resurser för krocksimuleringen. Utan denna kunskap blir det svårt för företaget att säkerställa kontinuiteten i simuleringen.

Kunskapen om hur kritiska resurser kan påverka företagens förmåga att utföra en aktivitet är central.

Den maximalt tolerabla avbrottstiden som bör ställas för en aktivitet avgör kraven på återhämtningstid för de kritiska resurserna (ofta med en säkerhetsmarginal i förhållande till den maximalt tolerabla avbrottstiden). Med detta menas den tid inom vilken dessa resurser måste kunna återgå till normal funktion efter ett avbrott.

En beroendeanalys kan innefatta följande moment:

- Identifiera kritiska beroenden i form av interna och externa resurser (personal, system, utrustning, leverantör, funktion, tjänst etc.) för de kritiska aktiviteterna.
- Definiera krav på återhämtningstid, men också krav på tidpunkt då arbetet måste kunna återställas, för varje resurs.[16]

[16] Den engelska benämningen för kravet på återhämtningstid är Recovery Time Objective, RTO. Även Recovery Point Objective, RPO, är ett väsentligt krav i detta sammanhang för att säkerställa färskheten i det för aktiviteten nödvändiga arbetsmaterialet. I datalagringssammanhang bör exempelvis krav ställas rörande hur gammal data maximalt får vara för att medge funktionalitet i den kritiska aktiviteten.

Riskvärdering

I riskvärderingen identifieras, analyseras och utvärderas händelser och konsekvenser som kan störa kontinuiteten i kritiska aktiviteter.[17]

Fokus för riskvärderingen ligger i regel på resurser, de vill säga de resurser som krävs för att leverera aktiviteten. Händelser som kan störa kontinuiteten hos kritiska resurser kan vara externa eller interna. Exempel på sådana är elavbrott, sjukdom, tekniska eller mänskliga fel, sabotage och naturkatastrofer. De händelser och konsekvenser som är av intresse att analysera kan vara olika beroende på vilken kritisk resurs som studeras. Vid en riskvärdering inom ramen för kontinuitetsplanering tonas ofta betydelsen av en enskild händelses sannolikhet ned, till förmån för en analys av sannolikheten att en kritisk resurs inte kan användas. Allt från extrema oväder till finansiella svårigheter kan till exempel påverka leveranserna av komponenter från en underleverantör.

Se generellt på riskvärderingen!
Hur stor är exempelvis sannolikheten att en underleverantör inte kan leverera, oavsett vilken händelse som orsakar avbrottet?

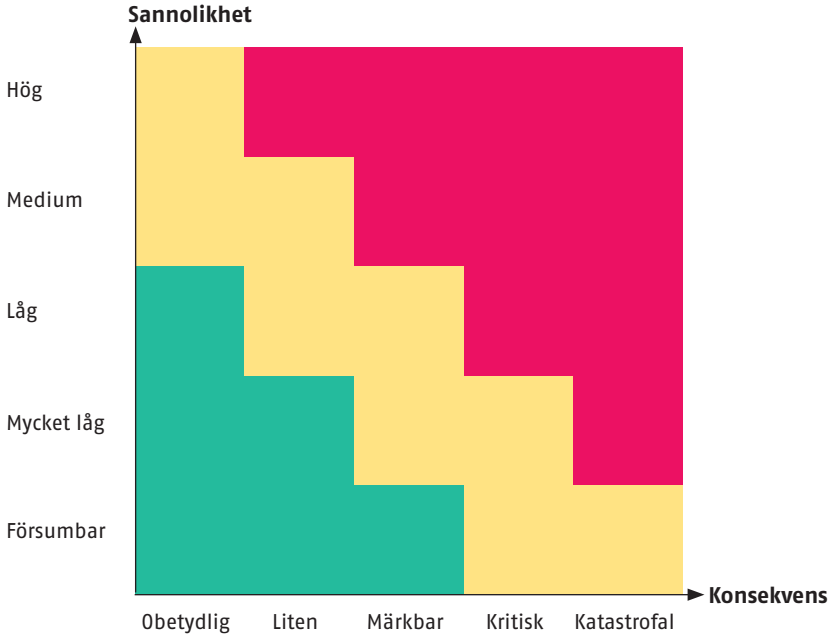
Då den möjliga konsekvensen av en händelse analyseras bör hänsyn tas till resultatet av affärskonsekvensanalysen. Om konsekvensen innebär att en kritisk resurs, till exempel ett system, inte fungerar så vet vi att en kritisk aktivitet påverkas och att ett avbrott i en kritisk aktivitet efter en viss tid får en icke tolerabel påverkan på en kritisk process. I exemplet med krockkuddestillverkaren vet företaget att ett avbrott på mer än åtta timmar i krocksimuleringen skapar konsekvenser för produktutvecklingsprocessen som inte bedöms som tolerabla. För de händelser, exempelvis elavbrott, som bedöms kunna inträffa med betydande

[17] I begreppet konsekvens inkluderas här de sårbarheter som finns i verksamheten och dess omgivning. Genom dessa sårbarheter kan en händelse orsaka en specifik konsekvens. Det finns en mängd olika verktyg, modeller och metoder tillgängliga för att genomföra delar av eller hela arbetet med riskvärdering. Valet av verktyg, modell eller metod bör göras mot bakgrund av tillgängliga resurser samt i relation till de risker och den verksamhet som utgör analysobjektet i varje enskilt fall.

sannolikhet, bör den verkliga återhämtningstiden för resurserna identifieras. Uppfylls de krav som definierats i affärskonsekvensanalysen? Är risken liten eller stor? Kan risken accepteras? Behöver risken minskas eller kan mer risk tas? På så vis sker en systematisk riskvärdering av samtliga kritiska resurser.

Riskvärderingen kan omfatta följande moment:

- **Riskidentifiering:** Identifiera händelser som kan påverka kontinuiteten hos de resurser som stöder aktiviteterna!
- **Riskanalys:** Analysera konsekvenser och sannolikhet. Konsekvensen bedöms med hänsyn tagen till de maximalt tolerabla avbrottstider för varje kritisk aktivitet som definierats i affärskonsekvensanalysen!
- **Riskbedömning/Riskutvärdering:** Bedöm vilka risker som inte kan accepteras liksom var det finns onödig redundans enligt acceptanskriterierna!



Riskmatrisen i sin enklaste form kan användas för att analysera och bedöma riskerna hos kritiska resurser.

Kontinuitetsstrategi

I en kontinuitetsstrategi formuleras grundläggande principer för hur företaget avser uppnå de krav på kontinuitet som definierats i de inledande stegen.

Affärskonsekvensanalysen och riskvärderingen skapar viktig kunskap om vad som är kritiskt i verksamheten och vilka risker dessa delar av företaget är exponerade mot. Denna kunskap bör omsättas i lämpliga strategier, lösningar och planer genom vilka företaget kan optimera sin robusthet och sin förmåga att hantera störningar och avbrott i verksamheten.

En kontinuitetsstrategi beskriver i regel hur företaget tänker sig att uppnå kontinuitet. Fokus ligger på verksamhetens viktigaste områden. Det kan exempelvis röra sig om kompetens, leverantörer, system och produkt- eller tjänsteklassificeringar. Inom området kompetens kan kontinuitetsstrategin för vårt krockkuddeföretag, som är extremt beroende av ett par nyckelpersoner, vara kompetensspridning. Inom systemområdet kan strategin visa på huruvida kontinuiteten ska uppnås genom redundanta lösningar vid varje arbetsplats, alternativt genom att geografiskt omfördela arbetsuppgifter mellan arbetsplatser i händelse av avbrott vid en av dem. Idag är det även vanligt att en strategi behandlar produkt- och tjänsteklassificeringar baserat på en produkt eller tjänsts finansiella betydelse för företaget.

Många gånger finns grunderna till en kontinuitetsstrategi redan innan en affärskonsekvensanalys och en riskvärdering genomförts.

De kunskaper som de inledande stegen ger företaget skapar förutsättningar att utveckla, optimera och tydliggöra kontinuitetsstrategin. Resultatet från riskvärderingen kan till exempel visa att de verkliga riskerna i företagets kritiska processer handlar om bristen på viktig kompetens. En strategi med fokus på att skapa en redundant systeminfrastruktur kommer inte att hantera denna risk. Istället kanske fokus bör ligga på kompetensförsörjningen. Möjligen bör anställningsvillkoren för nyckelpersoner förändras för att minska personalomsättningen och göra tjänsterna mer attraktiva vid nyrekrytering.

Kontinuitetslösningar

Utifrån en beslutad kontinuitetsstrategi definieras förslag till kontinuitetslösningar.

Kontinuitetslösningarna kan omfatta nödvändig organisationsutveckling, investeringar i reservlösningar och allokering av resurser för att kunna återställa verksamheten efter ett avbrott. Det kan exempelvis röra sig om omorganisering av en viss enhet inom företaget eller införande av ett nytt reservalternativ för ett av företagets IT-system. Andra lösningar kan vara upphandling av alternativa leverantörer eller etablering av en reservanläggning dit delar av företaget kan flytta vid en incident eller kris.

Varje enskild lösning bör utvärderas mot bakgrund av huruvida den är kostnadseffektiv. Bedömningen görs genom att lösningens reducering av återhämtningskostnaden uppskattas.[18] Genom att ställa denna kostnadsreduktion mot den totala investeringskostnaden för lösningen kan ett ROI-värde (Return of Investment) beräknas.[19] Detta ger ett bra underlag när ledningen ska fatta beslut om kostnadseffektiva kontinuitetslösningar.

Kontinuitetslösningar kan vara av olika komplexitet och storlek. Vissa kan ta några månader att införa, exempelvis inköp av nya reservsystem. Andra kan kräva särskilda åtgärdsplaner och ta flera år att genomföra, såsom upprättande av nya reservlokaler eller utveckling av en specifik kompetens.

[18] Det vill säga reduktionen i kostnaden för ett avbrott, från det att avbrottet inträffar tills dess att full normal verksamhet är återtagen tack vare kontinuitetslösningen.

[19] Return Of Investment – nyttan av en investering i jämförelse med investeringskostnaden (en teoretiskt bättre, men mer avancerad metod innebär att Value at Risk (VAR) används för bedömning av kostnadsbesparingen).

Kontinuitetsplan

Reserv- och återgångsrutinerna dokumenteras i en kontinuitetsplan.

Kontinuitetslösningarna kan behöva kompletteras med reserv- och återgångsrutiner. Rutinerna aktiveras för att upprätthålla en kritisk aktivitet och för att göra en snabb återgång till normal verksamhet möjlig. Reserv- och återgångsrutinerna kan innehålla checklistor liksom definitioner av ansvar, roller och befogenheter. Rutinerna dokumenteras i regel i det som kallas en kontinuitetsplan.

Om kontinuitetslösningen utgörs av en reservbyggnad dit företaget kan flytta vid en kris, bör den aktuella personalen känna till hur byggnaden ska användas. Man bör fastställa rutiner för hur flytten dit ska ske och vilka särskilda rutiner som gäller under vistelsen på den nya platsen. Om kontinuitetslösningen avser reservsystem bör rutiner finnas för hur och när det ska aktiveras. Det kan alltså i ett stort företag finnas ett stort antal kontinuitetsplaner och det är viktigt att dessa är synkroniserade med varandra. Information om hur en specifik kontinuitetsplan aktiveras kan även ingå i en krishanteringsplan.

Krishanteringsplan

I en krishanteringsplan beskrivs de övergripande rutiner som styr ledningens hantering av krisen.

Krishanteringsplanen kan innehålla information avseende företagets krisledning, krishanteringsorganisationen, mandat och ansvar, samverkan (med kommun, företag, organisationer och liknande), krisstödsrutiner, kriskommunikation, personalhantering med mera. Det vill säga all den information som en ledningsorganisation finner nödvändig för att snabbt och effektivt kunna verka i en krissituation eller i en situation som kan tänkas utvecklas till en kris.[20] Krishanteringsplanen bör kontinuerligt stämmas av med relevanta kontinuitetsplaner för att säkerställa att dessa fungerar effektivt tillsammans.

[20] Varje företag bör ha definierat vad en kris innebär för den egna verksamheten.

Utbildning, övning och revision

Att öva och testa de implementerade kontinuitets- och krishanteringsplanerna för att säkerställa att de fungerar är en viktig del av det kontinuerliga arbetet.

Kontinuitetsplanering bör vara en del av det dagliga arbetet och företagskulturen. Detta ställer krav på såväl tydliga mål inom företaget som ett utbildningsprogram för att skapa kunskap och förståelse kring de metoder och verktyg som stödjer genomförandet av de olika komponenterna.

Oberoende av hur väl utformad och genomtänkt en kontinuitetsstrategi eller en kontinuitetsplan är bör övningar genomföras för att identifiera brister som kräver verksamheternas uppmärksamhet. Krisövningar och tester kan förbättra efterlevnaden av såväl som innehållet i kontinuitets- och krishanteringsplanerna.

Revision är ett sätt att försäkra sig om företagets kontinuitet i affärskritiska processer, aktiviteter och resurser. Revisionsarbetet kan innebära att:[21]

- validera huruvida kraven på kontinuitet fortfarande är aktuella.
- validera kontinuitetslösningar.
- validera kontinuitetsplaner.
- verifiera att övning, utbildning och uppföljning av aktiviteter sker i nödvändig omfattning.
- identifiera svagheter och behov av åtgärder i företagets kontinuitetsplaneringsprogram och att säkerställa förbättringsåtgärder.

[21] BCI, Business Continuity Institute (2005), Good Practice Guidelines – A framework for Business Continuity Management, www.thebci.org

Kultur och uppföljning

Kontinuitetsplaneringsprocessen blir effektiv då den utgör en del av företagskulturen.

Att inom ett företag utveckla en kultur för kontinuitetsplanering kräver en engagerad ledning. Den bör aktivt kommunicera vikten av att de rutiner som stödjer kontinuitetsplaneringen efterlevs och att metoden verkligen tillämpas. Detta kan kräva särskilda insatser för att främja utvecklingen av en "kontinuitetskultur". Insatserna kan omfatta följande tre steg:[22]

1. Utvärdera befintlig nivå på kunskap och engagemang avseende kontinuitetsplanering mot de mål som etablerats inom företaget.
2. Initiera ett arbete för att skapa de färdigheter, den kunskap och det engagemang som krävs för att kontinuitetsplaneringen skall bli framgångsrik.
3. Följ upp resultaten från kampanjen!

Det är viktigt att definiera tydliga mål för företagets arbete med kontinuitetsplanering, inte minst för att kunna mäta resultat och framsteg. Implementeringen av beslutade kontinuitetslösningar, liksom efterlevnaden av befintliga kontinuitets- och krishanteringsplaner, kan också kontinuerligt följas upp av ledningen genom benchmarking.

[22] BCI, Business Continuity Institute (2005), Good Practice Guidelines – A framework for Business Continuity Management, www.thebci.org

Standarder

Det finns en mängd olika standarder tillgängliga som kan underlätta arbetet med kontinuitetsplanering. För dig som önskar ta del av dessa standarder så går det bra att vända sig till respektive lands standardiseringsinstitut alternativt till den svenska motsvarigheten, SIS[23], för mer information.

- Storbritannien: BS 25999-1 Code of practice for business continuity management (ersätter PAS 56)
- USA: NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs (2004 Edition)
- Australien: AS/NZS HB221:2004 Business Continuity Management
- Singapore: TR19:2005 Business Continutiy Mananagement
- ISO/IEC 17799:2005 Information technology – security techniques – Code of practice for information security management

Länkar

Det finns ett stort antal informationskällor på Internet för den som vill veta mer om kontinuitetsplanering och dess senaste utveckling och tillämpning. Två intresseorganisationer är särskilt användbara för den som är intresserad av eller verksam inom kontinuitetsplanering:

The Business Continuity Institute
http://www.thebci.org

The Disaster Recovery Institute – International
http://www.drii.org

[23] Swedish Standards Institute
http://www.sis.se/DefaultMain.aspx

Kontinuitetsplanering skapar kunskap om hur företag på ett kostnadseffektivt sätt kan förebygga och begränsa konsekvenserna av avbrott i verksamhetens kritiska processer och aktiviteter.

Genom att omsätta denna kunskap i strategier, lösningar och planer bidrar kontinuitetsplanering till att öka ett företags förmåga att leverera tjänster och produkter i samband med oplanerade avbrott och kriser.

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

Tel 08 593 710 00
Fax 08 593 710 01

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se