

Checklista

Kontinuitets- och katastrofåterställningsplan

Här är stegen för att komma igång med ditt arbete.



“ Planen är en trygg hamn i den digitala stormen!

- Lena Graungaard Lindahl

Introduktion

Den här checklistan är baserad på artikeln som jag har skrivit om BCA. Den finns på secify.com/kunskapscenter. Checklistan är framförallt för dig som är i startgröparna för ditt kommande kontinuitetsarbete.

Ett tips innan du börjar. Ha inte för höga ambitioner om du inte tidigare har erfarenhet från liknande arbete. Det är lätt hänt att man gör ett för stort arbete och fastnar. Då är det bättre att slutföra ett mindre arbete och därefter, med den kunskap och erfarenhet som man fått, bygga upp ett större från grunden.



Lena Graungaard Lindahl
Rådgivare inom informationssäkerhet

Förarbete

Affärskonsekvensanalys:

- Börja med att identifiera din organisations mest kritiska affärsprocesser och aktiviteter tillsammans med nyckelpersoner från olika avdelningar. Koppla kritiska aktiviteter och processer till tillgångar (som den kritiska aktiviteten/processen är beroende av) och koppla dessa till kritiska affärsaktiviteter. Glöm inte bort era personalresurser.
- Fundera över hur länge varje affärsprocess/aktivitet och kritisk resurs kan vara otillgänglig. Vad är den maximala tolerabla avbrottstiden? Vad är maxtiden ni har på er att återställa en tjänst efter ett driftsstopp (RTO)? För kritiska IT-resurser, bedöm även den mängd data som ni kan förlora vid en oförutsedd händelse (RPO).
- Bedöm konsekvenserna av olika avbrottstider för att avgöra vad som är acceptabelt.

Riskhantering:

- Med kunskapen om vad som är viktigt för företaget ska du nu försöka identifiera och analysera vilka risker som kan finnas och hur stor sannolikheten är att ni kan återställa aktiviteten/processen och beroende resurser inom tolerabel avbrottsid.
- Identifiera potentiella hot mot kritiska processer, aktiviteter och kritiska resurser.
- Analysera riskerna baserat på konsekvens och sannolikhet. Vad blir konsekvenserna om risken inträffar och hur stor är sannolikheten att ni inte klarar av att återställa inom tolerabel avbrottsid? Vad har ni för befintlig redundans.
- Bedöm vilka risker som inte kan accepteras och kräver åtgärder.



Planerna

Business Continuity Plan (Kontinuitetsplan):

- Utveckla en plan för att säkerställa att kritiska aktiviteter och processer kan fortsätta på en acceptabel nivå under en störning, så kallade "reservrutiner".
- Identifiera alternativa resurser och platser för att möjliggöra kontinuitet vid störningar.
- Skapa flexibilitet och realistiska alternativ i planen för olika scenarier.
- Säkerställ kommunikationsvägar och kontaktpersoner för intern och extern kommunikation.
- Ta fram tydliga roller och ansvar i händelse av en störning "Business Continuity Team".
- Ta fram en prioriteringsordning för kritiska aktiviteter/processer och resurser utifrån Affärskonsekvensanalysen.



Disaster Recovery Plan (katastrofåterställningsplan):

- Ta fram en prioriteringsordning för kritiska IT-resurser utifrån Affärskonsekvensanalysen.
- Ta fram roller och ansvar i händelse av störning "Disaster Recovery Team".
- Ta fram återhämtning och återställningsrutiner av data och system.
- Ta fram backuprutiner.

Efterarbete

Testa, revidera och utbilda:

- Planerna ska godkännas av ledningen.
- Testa regelbundet och utvärdera planerna för att identifiera och åtgärda brister och förbättringar.
- Uppdatera planerna med hänsyn till förändrade förhållanden och lärdomar från tidigare incidenter.
- Utbilda personalen regelbundet om användningen av planerna och deras roller och ansvar.

