Så skyddar du ditt datacenter

5 Steg för att få strategi och tjänster på plats

Varje företag behöver en strategi för hur de ska agera vid avbrott i de it-system som hela verksamheten är beroende av. Katastrofåterställning som tjänst är ett kraftfullt och flexibelt verktyg för att realisera en sådan strategi – oavsett storlek hos företag.

Med allt fler och allt mer komplexa cyberattacker står varje företags datacenter under ständigt hot. Lägg också till utvecklingen mot fler extrema vädersituationer och läget blir knappast bättre. Samtidigt blir företaget och kunder mer beroende av just datacentret, de applikationer som körs där och den information som lagras i det. Ett avbrott skadar inte bara verksamheten direkt, utan påverkar också kundernas förtroende för företaget.

Få företag har idag råd med avbrott i sina datasystem. Därför skapar större organisationer strategier och handgripliga planer för hur de ska agera vid stillestånd i it-systemen. För vissa organisationer är sådana så kallade kontinuitetsplaner till och med lagstadgade.

Vi på Atea som jobbar med katastrofsäkring och datacenter ser att följande steg är till stor nytta för att få en hållbar strategi och rätt tjänster på plats.

1 Upprätta en strategi och kontinuitetsplan

1

Upprätta en strategi och kontinuitetsplan

Oavsett hur kraven utifrån ser ut och oavsett hur stort företaget är bör alla organisationer upprätthålla en kontinuitetsplan. Konsekvenserna av en cyberattack eller annan incident kan helt enkelt bli större än verksamheten mäktar med.

Avbrott i företagens it-system kostar inte bara stora summor pengar utan riskerar också att skada kundernas förtroende för företaget. Slutanvändares förväntningar på att digitala tjänster och information ska vara omedelbart tillgängliga ökar hela tiden. När det gäller de direkta ekonomiska konsekvenserna är det inte bara det faktum att system och information inte är tillgängliga som orsakar skador. En stor kostnadsdrivare är också den mängd information som inte kan skapas under avbrottet – att produktionen ligger nere med andra ord.

Strategin eller kontinuitetsplanen för minimering av de skador it-incidenter kan ge upphov till är den ryggrad som utformningen av alla åtgärder, system och funktioner ska utgå från.

2 Överväg externt stöd för utformning av planen

2

Överväg externt stöd för utformning av planen

Att upprätta en strategi är inte särskilt svårt men blir snabbt komplext. Exempelvis behöver företaget klassa olika typer av information och applikationer, för att kunna prioritera rätt när de tekniska lösningarna utformas. Därför är det en god idé att ta hjälp av någon med stor erfarenhet av den här typen av uppgifter.

3 Undvik punktinsatser

3

Undvik punktinsatser

Som en del av sin kontinuitetsplanering upprättar stora bolag ofta en reservdatahall som tar över vid ett eventuellt avbrott. Det är en sund åtgärd men sällan något som mindre företag har råd att göra.

Resultatet hos dessa blir inte sällan ett lapptäcke av punktåtgärder, som att säkerhetskopiera viss data och vissa applikationer, men inte nödvändigtvis på samma ställe eller med samma verktyg. Sådana åtgärder hjälper bara delvis, i bästa fall. I många krissituationer knappast alls. När huvudsajten går ner tar det allt för lång tid att starta upp den igen, läsa in säkerhetskopior på rätt ställen och återställa applikationer.

En sådan lösning kan i praktiken inte möta kraven i en robust kontinuitetsplan.

4 Dubblera datahallen i molnet

4

Dubblera datahallen i molnet

En egen dubblerad datahall är inte det enda sättet att säkerställa tillgängligheten hos it-systemen. Det finns en annan väg att välja för att undvika eller minimera avbrott i produktionen vid cyberattacker eller andra incidenter.

Med Disaster recovery som tjänst kan företag av alla storlekar inte bara spegla valda resurser i sitt datacenter och få tillgång till dem inom bara några minuter efter ett oplanerat avbrott. Tjänsten skapar också en hög grad av flexibilitet vilket gynnar såväl kostnadsbilden som säkerheten.

I praktiken blir en sådan tjänst en del av det befintliga datacentret. Alla ändringar som görs exempelvis i form av nya eller uppdaterade applikationer och utökade lagringsresurser, återspeglas i tjänsten. I praktiken kan den betraktas som en reservdatahall i molnet.

Växlingen från den egna datahallen till den speglade versionen kan ske på bara några minuter. Men det sker inte automatiskt vid avbrott, utan är något som måste väljas aktivt. Detta då beslutet att stänga den egna datahallen och gå över till reservsajten är något som påverkar affären. Därför måste det finnas en strategi och en plan som beskriver när och av vem beslutet ska tas.

5 Håll isär verktyg och strategi

5

Håll isär verktyg och strategi

Det är viktigt att förstå att Disaster Recovery som tjänst bara är ett kraftfullt verktyg i realiserandet av strategin. Genom att tjänsten kopplas så tätt samman med företagets befintliga datacenter blir det också relativt enkelt att utforma och följa en sådan.

SAMANFATTNING

Företag utsätts idag för fler och mer komplexa hot mot sina datahallar än någonsin, bland annat som ett indirekt resultat av digitaliseringen. Lyckligtvis har den utvecklingen även medfört att skydden har kunnat göras betydliga effektivare, mer flexibla och kostnadsmässigt mer fördelaktiga. Disaster recovery som tjänst är ett av dessa skydd och bör betraktas som en naturlig del av varje datahall, då risken för längre avbrott helt elimineras.

Vill du veta mer om Disaster Recovery som tjänst?

Ring eller maila Natalie Yilmaz på natalie.yilmaz@atea.se alt.
08-477 48 83

6 steg mot katastrofsäkring i molnet

1. Finns det en befintlig kontinuitetsplan framtagen inom företaget? Börja i så fall med att gå igenom den och se vad som kan återanvändas. Om inte, upprätta en ny kontinuitetsplan.

2. Identifiera vilka system som är affärskritiska och vilken information som behöver skyddas för att garantera att verksamheten i företaget kan fortsätta vid en störning.

3. Skapa återstartsplaner för de kritiska systemen och de system och den information som behöver skyddas.

4. Använd Ateas disaster recovery som tjänst för att tekniskt möjliggöra de återstartsplaner och det informationsskydd som ni identifierat under ovanstående punkter.

5. Öva på vad som händer vid en störning. Gå igenom kontinuitetsplanen och träna på att flytta resurser mellan det egna datacentret och Ateas datahall i molnet.

6. Kommunicera lagd plan till verksamheten så att de vet vilka system som de kan förvänta sig vara tillgängliga och med vilken kapacitet och prestanda man kan fortsätta att bedriva verksamheten under en störning.