6 vragen aan de Servicedesk

Disaster Recovery

1. Ernstige calamiteiten; hoe bereid ik mijn organisatie voor?

Uw organisatie is het doelwit van verlammende cyberaanvallen of krijgt te maken met brand, een aardbeving of andere natuurrampen… Hoe te handelen in een dergelijke situaties?

Om de continuïteit van de belangrijkste bedrijfsprocessen zo min mogelijk te onderbreken, de belangrijkste data veilig te stellen en de meest kritische apparatuur weer in de lucht te krijgen maken we een disaster recovery plan (DR-plan). Hierin staan antwoorden op vragen als: Wie moeten we informeren? Hebben we een noodaggregaat? Wie heeft de toegangscodes van onze cloudomgeving in beheer?
Verder omvat het plan onder meer voorzorgsmaatregelen, beschrijvingen van configuraties, instellingen, vormen van back-up van data en een concrete planning van te nemen acties in het geval van bijvoorbeeld blikseminslag.

2. Hoe breng ik de impact van een calamiteit in kaart?

Om een startpunt voor een disaster recovery plan te bepalen bekijken we de continuïteit van de organisatie eerst in zijn geheel. Vervolgens worden ook de risico's in kaart gebracht en het besluit hoe hier mee om te gaan.

De meeste organisaties beschikken over een continuïteitsplan voor hun business. Hierin staat onder meer een beschrijving van de belangrijke bedrijfsprocessen en hun statistieken uitgedrukt in bijvoorbeeld een Recovery Point Objective (RPO) en Recovery Time Objective (RTO). De RPO en RTO staan tezamen voor het herstelpunt en de hersteltijd. Deze bedrijfsprocesstatistieken zijn toegewezen aan de onderliggende ICT-systemen en -infrastructuur die de processen in hun uitvoering ondersteunen.

3. Waaruit bestaat een goed DR-plan?

In een DR-plan zijn de processen gedocumenteerd die de ICT-infrastructuur beschermen tegen een calamiteit. Het plan beschrijft per ICT-systeem welke stappen er moeten worden genomen om het systeem in geval van een calamiteit te kunnen herstellen. Verder is benoemd welke personen en afdelingen onderdeel zijn van het DR-team. Omdat geen enkele organisatie hetzelfde is, wordt het DR-plan op maat, volledig toegespitst op de organisatie geschreven.

4. Welke factoren bepalen de recovery strategie?

Allereerst dient uiteraard vastgeseld te worden welke risico's afgedekt moeten worden. Zodra de RTO- en RPO-metrics zijn toegewezen aan de ICT-infrastructuur, kan de DR-planner de meest geschikte recovery-strategie voor elk systeem bepalen.
Uiteindelijk bepaalt de organisatie het ICT-budget en dus de RTO- en RPO-metrics die bij het beschikbare budget moeten passen. Geen gegevens- en tijdverlies is wat de meeste managers willen. De praktijk wijst vaak uit dat dit kostentechnisch onhaalbaar is. Solipsis Managed Services zet de gewenste beschikbaarheid van de oplossingen en het hoge niveau van bescherming van data naast elkaar en denkt met u mee.

5. Wat houdt een uitwijk in?

Als vanwege een calamiteit de primaire ICT-omgeving niet beschikbaar is, kan door middel van een uitwijk gebruik worden gemaakt van een andere locatie om de bedrijfskritische functies op te starten. De alternatieve locatie en de faciliteiten die daar aanwezig moeten zijn worden in ieder geval opgenomen in het DR-plan.

6. Is er tenslotte nog een tip?

Een calamiteit van onvoorziene omvang vraagt om een goed voorbereide, geteste en vastgelegde aanpak. Onvolledige RTO's en RPO's kunnen leiden tot vertraging in de oplossing en kunnen de impact van de calamiteit verlengen en sterk vergroten. Statistieken uit de verzekeringswereld leveren hierover een ontluisterend beeld op. Een DR-plan functioneert pas goed als het minimaal een keer per jaar getest en waar nodig bijgesteld wordt.

Wilt u meer informatie over ICT-rampbestrijding? Solipsis Managed Services heeft ervaring met organisaties en rampen van aanzienlijke omvang. Neem contact op een van onze adviseurs: (088) 599 16 08.