infotechnology

Oorzaken en gevolgen van ongeplande downtime

12 methoden om de kans te verkleinen en de gevolgen te beperken

Een white paper van RAM Infotechnology

16-01-2012

infotechnology

Introductie

Ongeplande downtime is de tijdsduur waarop een netwerk of een component niet te gebruiken is door een onverwachte oorzaak. Deze white paper gaat in op de oorzaken en gevolgen en bespreekt 12 methoden om ongeplande downtime te voorkomen of de schade te beperken. De informatie in deze white paper stelt organisaties in staat de risico's van ongeplande downtime in te schatten en keuzes te maken bij het kiezen van oplossingen.

Uit het onderzoek 'Disaster Recovery' van IT-dienstverlener EMC (zie kader) blijkt dat 75% van de bedrijven vreest voor het voortbestaan na een ramp waarbij IT verloren gaat. Meer dan 50% van de bedrijven raakt jaarlijks data kwijt na uitval van systemen. Ongeplande downtime is dus voor iedere bedrijfsvoering een belangrijk onderwerp.

Kenmerken van downtime

Ongeplande downtime, stroomstoringen en andere (menselijke) fouten komen dagelijks voor. De kenmerken van ongeplande downtime:

- Komt altijd onverwacht;
- Breekt direct lopende processen af;
- Data gaat verloren, maar niet duidelijk is welke data;
- De oorzaak is onbekend en vraagt dus meer tijd om op te lossen;
- Niemand kan direct zeggen wanneer de downtime voorbij is;
- De tijdelijke stilstand van medewerkers kost geld;
- De trage en onvolledige ("we weten het nog niet") communicatie over de problemen irriteert klanten en medewerkers;
- Via social media verspreiden negatieve berichten over downtime zich snel.

Herkennen en rapporteren

Wanneer ongeplande downtime regelmatig voorkomt, is het belangrijk om hierover goede rapportages bij te houden, zodat gerichte maatregelen mogelijk zijn en het effect ervan goed te meten is. Een probleem bij het rapporteren is dat calamiteiten onvoldoende opvallen ("het

hoort erbij"), niet gemeld worden ("bij wie?") of niet genoteerd worden (IT-afdeling verdoezelt haar eigen fouten). Zorg in die gevallen voor een interne procedure die alle betrokkenen stimuleert calamiteiten direct en duidelijk te melden.

Schade

Veel bedrijven geven aan failliet te gaan als ze 24 uur zonder IT komen te zitten.

- Is na 24 uur bijvoorbeeld duidelijk hoeveel data verloren is gegaan?
- En vanaf welk moment data verloren is gegaan?
- Zijn hierover rapportages beschikbaar en kan iemand die interpreteren?
- En is het dataverlies te herstellen?

De schade die ongeplande downtime kan opleveren is divers. Medewerkers en gebruikers van informatiesystemen kunnen niet of beperkt verder werken. Productie en logistiek vallen stil. Erger is het wanneer medische dossiers onbereikbaar worden en de gezondheid van patiënten in het geding komt. De zorgbranche stelt niet voor niets hoge eisen aan de beschikbaarheid van ICT. Bij ongeplande downtime van administratieve systemen treedt er snel achterstand op in de administratie, kunnen klanten niet geholpen worden en kunnen orders verloren gaan of arriveren leveringen te laat op hun bestemming.

Een grote schadepost zijn de extra uren voor overwerk of het inhuren van extra mankracht om achterstanden in te halen. De schade van verlies van data is moeilijk in te schatten, maar kan snel oplopen. Bovendien bestaat de kans op schadeclaims van klanten of gebruikers van systemen wanneer zij door downtime niet kunnen voldoen aan hun verplichtingen. Tot slot kan er flinke imagoschade optreden bij klanten, potentiële klanten en medewerkers. Zeker wanneer downtime vaker voorkomt.

Twee of meer systemen

Veel organisaties maken gebruik van twee of meer systemen met gescheiden opslag van patient-, klant- en procesgegevens, waarbij volop uitwisseling tussen die systemen plaatsvindt. Bij ongeplande downtime is het zeer belangrijk om na te gaan welke gegevens er (nog) zijn.

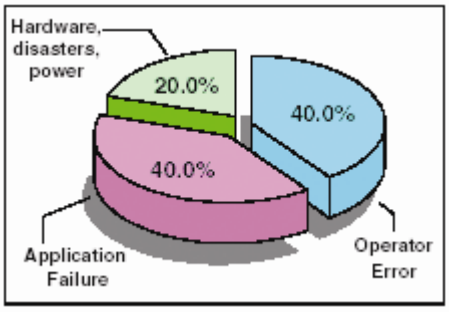
Vooral wanneer maar één systeem is down gegaan en het andere niet, kunnen er na de restore verschillen optreden. Dat kan bijvoorbeeld direct gevolgen hebben voor bestellingen en facturatie.

Oorzaken van ongeplande downtime

Oorzaken van een ongeplande downtime zijn een crash of een defect, veroorzaakt door mensen falen of door systemen.

Ongeplande downtime heeft drie hoofdoorzaken:

1. Hardware problemen en stroomstoringen
2. Applicatiefouten
3. Operatorfouten, menselijk falen



We kunnen deze oorzaken verder uitsplitsen naar storingen in hardware, rampen, stroomstoring, internet is uit de lucht, het geheugen zit vol, de serverload is te hoog, fouten in applicaties, incomplete upgrade of update, emergency maintenance (ongepland spoedonderhoud), diefstal, vandalisme en virussen.

Voor fouten van operators geldt vaak dat ze het gevolg zijn van onderbezetting of een gebrek aan voldoende kennis. Wanneer maar één persoon binnen de organisatie verantwoordelijk is voor uptime, nemen de risico's snel toe.

Zorgapplicaties leveren vaak problemen op, zeker na een upgrade, terwijl in de zorg juist een vlekkeloze werking verwacht wordt en meestal vereist is.

12 methoden om de kans te verkleinen en de schade te beperken

Ongeplande downtime is nooit volledig te voorkomen. Het is wel mogelijk om de kans erop te verkleinen en de schade te beperken. De volgende methoden hebben bewezen succesvol te zijn:

Kans op downtime verkleinen

1. Zorg voor een compleet redundante omgeving: power, servers, internet, systemen, storage, switches. De omgeving moet schaalbaar zijn om mee te kunnen groeien met de organisatie.

2. Kies voor fysiek gescheiden datacenters om de kans op downtime verder te verkleinen.

3. Pas zoveel mogelijk virtualisatietechnieken toe, zodat 'on the fly' onderhoud en uitbreidingen zijn door te voeren.

4. Bouw een OTAP-omgeving (Ontwikkel, Test, Acceptatie en Productie) om wijzigingen uitvoerig in de test- en acceptatieomgeving te testen voordat ze in de productieomgeving belanden. Upgrades van applicaties zijn een grote bron van ongeplande downtime.

5. Richt een NCC (Netwerk Control Center) in dat regelmatig systemen checkt en preventief onderhoud kan uitvoeren. Zij zorgen dat oranje signalen weer op groen springen en niet rood worden.

6. Doe minimaal jaarlijks een uitwijktest en check de procedures en contactpersonen.

Schade door downtime beperken

1. Zorg dat duidelijk is wie in actie moeten komen en wat de procedures zijn. Stel een DAP (Dossiers, Afspraken en Procedures) samen. Dit is klantspecifiek en gaat verder dan een SLA (Service Level Agreement).

2. Stel een disaster recoveryplan (onderdeel van DAP) op en test dit plan regelmatig.

3. Test periodiek gemaakte back-ups door ze terug te zetten en te controleren op inhoud en bruikbaarheid.

4. Maak gebruik van synchronisatie en snapshots om dataverlies te beperken.

5. Overweeg het gebruik van (schaalbare) Uitwijkservices die snel inzetbaar zijn bij ongeplande downtime.

6. Overweeg het gedeeltelijk of geheel uitbesteden van de primaire IT-processen aan een hosting provider die deze oplossingen standaard biedt en die voor een snelle restore zorgt. Een goede support is onmisbaar bij het oplossen van ongeplande downtime.

Back-up

Bedrijfsgegevens moeten snel beschikbaar zijn na een storing, brand of andere calamiteit. Het is belangrijk om interne back-up procedures regelmatig te checken. Check dan of alle data is teruggezet en of de data juist is. Zowel bij het opslaan als terugzetten van data kunnen er fouten optreden. Vergelijk de opgeslagen data dus met de originele data van voor de back-up. Als na een calamiteit ongemerkt verkeerde of verouderde data wordt teruggezet is de ramp nog veel groter.

Bij het gebruik van back-up services van een hosting provider, is het net zo belangrijk om de procedures en kwaliteit van de data na opslag en na restore regelmatig te controleren. Vraag om een uitgebreide rapportage van tests en van de ondernomen acties en resultaten in het geval van een ongeplande downtime.

Risicomanagement

Het voorkomen van ongeplande downtime brengt kosten met zich mee. Maak een afweging tussen deze kosten en de schade die kan optreden en de waarschijnlijkheid dat deze schade optreedt. Kijk ook naar de kostenverschillen tussen het zelf uitvoeren van maatregelen en het inschakelen van een hosting provider.

Naarmate de IT complexer wordt en de risico's groter is uitbesteden een betere optie, met name vanwege de reactietijd en oplostijd, de ervaring met het voorkomen van downtime en de schaalbaarheid van oplossingen.

Schaalbaar

Wanneer een organisatie groeit of verandert, en de IT meegroeit en mee verandert, is het zaak de maatregelen ter voorkoming van ongepland down gaan aan te passen en te toetsen aan de nieuwe situatie. Zeker wanneer de risico's groter worden (meer klanten, meer gebruikers, risicovollere toepassingen). Een schaalbare oplossing voor ongeplande downtime is dan gewenst. Daarbij draait het niet alleen om de hardware - met virtualisatie is hardware relatief makkelijk uit te breiden. Ook de procedures en contactpersonen moeten meegroeien. Uiteraard blijft het belangrijk om elke oplossing regelmatig te testen en aan te passen waar nodig. Vergeet dan niet om alle betrokkenen te informeren.

Samenvattend

Ongeplande downtime komt binnen organisaties vaker voor dan men denkt. Rapportages ervan ontbreken meestal. De schade die kan ontstaan is groot. Onderzoek toont dat aan. Ongeplande downtime is nooit te voorkomen, maar iedere organisatie kan maatregelen treffen om de kans te verkleinen. In deze white paper beschrijven we 12 methoden hiervoor. RAM Infotechnology heeft de kennis en middelen in huis om ongeplande downtime tot een minimum te beperken en de bedrijfsvoering snel te herstellen na hardwareproblemen, stroomstoringen, applicatiefouten, operatorfouten of ander menselijk falen.

infotechnology

Onderzoek: 75% bedrijven onzeker over herstart na ramp

Zeker driekwart van de Europese bedrijven is er niet zeker van na een ramp hun activiteiten te kunnen hervatten. De reden hiervan is dat ze niet in staat zullen zijn om hun data en systemen te herstellen.
Dit blijkt uit het onderzoek 'Disaster Recovery' van IT-dienstverlener EMC.

Meer dan 50% raakt data definitief kwijt na uitval systemen

Meer dan de helft van de 1750 ondervraagde Europese bedrijven geeft bovendien aan het afgelopen jaar gegevens te zijn kwijtgeraakt door het uitvallen van systemen. Bedrijven in de Benelux gaan daarbij aan kop. Zij hebben het meeste last van data-uitval en blijken het minste te besteden aan het veiligstellen
van data.

Belangrijkste oorzaken

De meeste problemen worden veroorzaakt door: het falen van hardware (61 %), uitvallen van de stroom (42 %) en falen van de software (35 %).

Back-up en recovery-strategieën herzien

Los van de oorzaak geeft 44 % van de ondervraagde organisaties wel aan dat ze hun procedures voor back-up en recovery hebben aangepast na een incident. EMC is er dan ook van overtuigd dat het voor veel bedrijven noodzakelijk is hun back-up en recovery-strategieën aan te passen.
Bron: PCM (24-11-2011)