Alta disponibilidade não é luxo.
Como eliminar o tempo de inatividade dentro das pequenas e médias empresas

A tecnologia da informação (TI) é ao mesmo tempo o ponto forte e ponto fraco das pequenas e médias empresas. Quando o alcance dessas empresas é mundial, há funcionários trabalhando a qualquer hora do dia e da noite e os negócios estão sempre acontecendo, por isso qualquer interrupção na disponibilidade dos aplicativos pode gerar perda de receita, do valor da marca e problemas de regulamentação. Em casos extremos, uma indisponibilidade mais prolongada pode ter implicações até fatais para a empresa.

Como a sua empresa tem então que se precaver contra esse tipo de ameaça tão evidente? O pior é que a maioria das empresas nem sabe como lidar com isso.

A continuidade dos negócios, ou seja, o planejamento, a preparação e a implementação de sistemas corporativos mais robustos antes que ocorra uma paralisação não programada, normalmente é considerada um problema de TI. A maioria das empresas acha que esse é um problema que tem que ser resolvido pelo departamento de TI. Essa atitude acaba levando à implementação de uma grande variedade de soluções que não seguem uma orientação estratégica. Mas na verdade, como o próprio nome diz, a continuidade dos negócios é um problema de negócios, que exige a conscientização da empresa como um todo.

Veja uma forma rápida de verificar se o seu plano de continuidade dos negócios está deixando sua empresa exposta:

- **Se o seu plano exige um grau alto de intervenção manual, sua empresa está exposta;**
- **Se o seu plano aceita perda de dados além de alguns segundos no caso de sistemas críticos, sua empresa está exposta;**
- **Se o seu plano não é capaz de recuperar o acesso aos sistemas críticos em uma questão de minutos, sua empresa está exposta;**
- **E se o seu plano depende de uma tecnologia de backup e recuperação de 30 anos atrás, sem dúvida sua empresa está exposta.**

Por 30 anos, o backup e a recuperação têm sido a técnica padrão para proteção dos sistemas de TI, mas que foi desenvolvida em uma época bem mais simples. O backup dos dados para fita ou disco ou a criação de instantâneos (o equivalente moderno do backup) cria uma imagem dos dados dos aplicativos em um determinado ponto no tempo. A recuperação a partir desse ponto não vai trazer nada além dos dados do backup mais recente. Seja a sua cópia de 15 minutos ou de dois dias atrás, recuperar um backup significa enfrentar as consequências da perda de dados. No caso de alguns sistemas isso pode não significar muito, mas no caso dos aplicativos mais críticos, a perda de dados pode ser catastrófica.

As técnicas de backup e recuperação foram desenvolvidas para processos computacionais relativamente não muito sofisticados, quando havia períodos programados em que ninguém estaria usando o sistema. Os aplicativos corporativos sempre ativos que você usa agora nas operações diárias precisam de uma tecnologia que garanta a disponibilidade contínua do sistema e elimine a ameaça da perda de dados, sem exigir uma janela de backup.

Na tecnologia moderna de alta disponibilidade (HA, high availability), as alterações nos aplicativos e nos dados são reproduzidas continuamente para um local remoto. Caso algo aconteça, seja um terremoto, uma pane de energia ou um problema em uma instalação de software, o failover para uma cópia atualizada do sistema ocorre de forma automática e imediata. A alta disponibilidade acaba com o tempo de inatividade e a perda de dados.

Alta disponibilidade para todos

A HA é a solução com que você sonhava para proteger seus sistemas contra paralisações e perda de dados. No entanto, ela foi evitada por muitos anos. A tecnologia era vista por muitos como complexa e cara demais para pequenas e médias empresas. O que se dizia era que só as grandes empresas com muito dinheiro e recursos de TI poderiam implementar soluções de HA. Isso continuou até recentemente.

Normalmente, a HA usa uma combinação de replicação e heartbeat do servidor para manter os sistemas de TI de um local remoto sincronizados com os aplicativos armazenados no data center principal. Antes, isso exigia redes dedicadas com alta largura de banda entre dois locais físicos e cópias redundantes do servidor, do armazenamento e do hardware de rede, com aplicativos e sistemas operacionais especiais. O custo dessa redundância sempre deixou a HA distante das empresas menores.

Hoje, as redes de baixo custo e alta largura de banda são tão comuns que viraram uma necessidade para todas as empresas. Além disso, diversos provedores de serviços oferecem servidores virtuais sob demanda por um baixo custo. Esses avanços na infraestrutura significam que a tecnologia de HA agora está disponível para mais empresas e por um valor bem mais acessível.

A enorme queda no valor dos custos da infraestrutura de HA colocou os planos de continuidade dos negócios de várias empresas em cheque. O data center está repleto de soluções de backup, normalmente descoordenadas e duplicadas. Se você dependia de backup e recuperação para a continuidade dos negócios, provavelmente já descobriu que essas soluções isoladas são um pesadelo em termos de manutenção, minam a produtividade e, acima de tudo, complicam a recuperação no caso de um desastre. As soluções de HA modernas oferecem um enfoque universal à continuidade dos negócios que reduz os custos da proteção de dados, simplifica a recuperação de desastres e elimina a perda de dados e a inatividade.

Figura 1 – Os riscos ocultos da complexidade quando se usa soluções de backup isoladas.

A HA pode ser indicada para a sua empresa, mas sem uma análise detalhada dos sistemas para determinar suas necessidades de recuperação, você não vai saber quais aplicativos serão beneficiados. O certo é que as restrições que limitavam a implementação de HA são coisa do passado. Você agora está livre para atender a outros assuntos relacionados aos seus planos de continuidade dos negócios.

As dez principais armadilhas em continuidade dos negócios

Todos falam sobre como fazer a recuperação de desastres do jeito certo, mas é bom saber também o que acontece se algo der errado no meio do caminho. Veja nossa análise das dez principais armadilhas no planejamento da recuperação de desastres e da continuidade dos negócios.

1 O foco deve ser a empresa e não a tecnologia!

A recuperação de desastres, a alta disponibilidade, o backup, a recuperação e a continuidade dos negócios têm o mesmo objetivo: manter as operações da empresa, independentemente das circunstâncias. É muito comum as empresas deixarem a tecnologia tomar as rédeas e ser o foco. Mas o que as pessoas se esquecem, e que é importante lembrar, é que a recuperação de desastres tem como objetivo atender a uma necessidade de negócios e que, portanto, tem sua base nos requisitos de negócios. Antes de tentar imaginar como implementar a recuperação de desastres, é preciso pensar nos motivos. Converse com os líderes da empresa para entender as prioridades deles. Para alguns é o e-mail, para outros é o sistema de entrada de pedidos on-line e há os que vão apontar o Microsoft SharePoint. Uma coisa é certa: você nunca vai saber quais sistemas são os mais importantes até perguntar para os usuários. Ao entender as necessidades da empresa, você vai conseguir estabelecer as prioridades que vão definir suas opções em termos de tecnologia de recuperação.

2 Pode ser uma catástrofe, ou não

Quando se pensa em recuperação de desastres, a primeira imagem que vem à cabeça são furações, enchentes, ataques terroristas e coisas do gênero, nunca uma atualização de software que não deu certo por um erro de procedimento ou de hardware em um equipamento de rede. É muito comum se planejar para uma situação mais grave e ser pego de surpresa por um erro trivial. Seu planejamento de recuperação de desastres precisa considerar todas as eventualidades, das básicas às catastróficas.

3 Como você pode definir uma verba se não sabe qual é o custo da inatividade?

O que mais acontece é que as empresas definem um valor em dinheiro para o planejamento da recuperação de desastres sem antes determinar o risco financeiro da inatividade e da perda de dados para os negócios. A menos que você consiga quantificar qual seria o seu prejuízo no caso de uma pane nos sistema críticos, será difícil afirmar o quanto você pode gastar para evitar esses prejuízos. Sua estratégia de recuperação de desastres precisa estar alinhada às necessidades dos negócios. Isso significa avaliar o custo financeiro da inatividade antes de alocar uma verba. Não se esqueça de incluir a conformidade com as regulamentações no cálculo das paralisações. Normalmente, há multas no caso de descumprimento de obrigações legais.

4 É preciso avaliar muito bem os riscos

Um evento que é considerado um desastre pode não ser visto da mesma forma por todos. Isso varia muito de uma empresa para outra, e até de um departamento para outro. Alguns eventos, como terremotos, são reconhecidamente catastróficos, o que deixa claro que uma empresa tenha que se proteger contra eles. Já outros podem ser comuns, como uma falha de hardware de rede, e podem ter um grande impacto financeiro. Ao pensar em recuperação de desastres, é importante perguntar: do que estamos tentando nos proteger? Não despreze o lugar comum. Os pequenos prejuízos decorrentes de problemas comuns acabam saindo caro.

5 Você tem um plano?

Se o seu plano de recuperação de desastres se resume a uma nota colada sobre as fitas de backup guardadas debaixo da cama do seu administrador de sistemas, as coisas vão mal. Pode parecer mentira, mas é grande o número de empresas que não possui um plano de recuperação de desastres. É fundamental desenvolver um documento formal detalhando todos os aplicativos, hardware, instalações, provedores de serviços, pessoal e prioridades, e que esse documento seja aprovado por todos os interessados dentro da empresa. É importante também que ele represente todas as áreas funcionais e traga orientações claras sobre o que acontece antes, durante e após um desastre.

6 Temos um plano, mas não testamos ainda

Um plano de recuperação de desastres só é útil se funcionar. A única forma de garantir que o seu plano vai funcionar é testando. E, para testar, é preciso simular condições reais de desastre, o que pode ser um desafio. Esses testes são caros, demorados e exigem que as pessoas envolvidas se ausentem das atividades diárias. Contudo, se não for feito um teste detalhado até o nível de aplicativos, é bem provável que você vá encontrar dificuldades durante um desastre real. Busque soluções de proteção dos dados que ajudem a criar ambientes para testes do seu plano sem interromper os negócios.

7 Quem é o responsável, e pelo quê?

Um desastre real pode ser uma situação caótica e confusa. Se as pessoas envolvidas não entenderem suas responsabilidades na recuperação de desastres, o processo de recuperação será longo e sujeito a problemas. Seu plano de recuperação de desastres precisa estabelecer claramente os papéis e responsabilidades de cada um dos envolvidos, e também o que fazer se pessoas importantes para o plano não estiverem disponíveis. Esses funcionários também deverão participar dos testes do plano de recuperação.

8 Ponto de recuperação? Tempo de recuperação?

É muito importante entender qual é o impacto da inatividade e da perda de dados para cada área da sua empresa. Essas informações definem a sua escolha em termos de tecnologia de recuperação, oferecem a base para o seu planejamento de recuperação de desastres e permitem que você saiba as consequências de uma falha na recuperação de cada aplicativo.

São usadas duas métricas para registrar a tolerância de um aplicativo à inatividade e à perda de dados: o objetivo de ponto de recuperação (RPO) e o objetivo de tempo de recuperação (RTO). Ambas são medidas em unidades de tempo. O RPO é contado para trás a partir do momento do desastre e RTO para a frente.

O RPO é uma medida de perda de dados. Quanto maior o RPO, mais o aplicativo consegue tolerar a perda de dados antes que se torne um problema para a empresa. Imagine-o como um ponto no tempo até o qual você consegue recuperar seus dados com sucesso. Todos os dados entre esse ponto e o momento do desastre não existem mais.

Já o RTO é uma medida da importância do aplicativo para as operações da empresa. Quanto menor o RTO, mais rápido você tem que trabalhar para fazer o aplicativo voltar a funcionar antes que o impacto na empresa comece a ficar significativo.

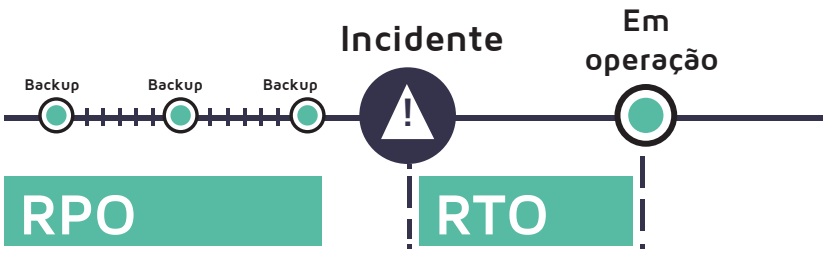

Figura 2 – Entender com que frequência deve ser feito o backup dos aplicativos e dados (Objetivo de ponto de recuperação – RPO) e com que rapidez você precisa recuperá-los (Objetivo de tempo de recuperação – RTO) é crucial para o seu plano de continuidade dos negócios.

Se você desconhecer o RPO e o RTO de cada aplicativo, você vai ficar em apuros na recuperação depois de um desastre. O que você fizer para garantir a recuperação após um desastre será meramente adivinhação. Com o RPO e o RTO você é capaz de definir o nível de serviço.

Tecnologias como a Proteção Contínua dos Dados são fundamentais para garantir que esses objetivos possam ser cumpridos.

9 A recuperação vai demorar mais do que você pensava

Para muitas empresas, o pensamento sobre a recuperação no caso de um desastre termina quando as fitas de backup saem do data center. Contudo, é fundamental entender quanto tempo levará para recuperar sistemas corporativos importantes e qual o volume de dados que será perdido após um desastre. Mesmo que você possa acessar as cópias de backup fora da empresa, isso não garante que a recuperação possa acontecer em tempo hábil. Você tem acesso a equipamentos que conseguem ler esses dados? Você consegue restaurar os dados e recriar os aplicativos com a rapidez que os usuários corporativos desejam? Você tem largura de banda suficiente para recuperar os dados a partir de um provedor de serviços em nuvem? Entender quanto tempo vai demorar para recuperar os aplicativos e o efeito da inatividade nos negócios pode levar você a ter que optar por outras tecnologias.

10 Voltando para casa

A volta para casa depois de um failover para um local de recuperação é uma opção que normalmente é desconsiderada no planejamento da recuperação de desastres. É fácil saber o porquê. Quando pensamos em desastre, pensamos somente em proteger os ativos valiosos. Pouco se pensa no que acontecerá com esses ativos depois que o desastre passar.

A capacidade de fazer o failback para os sistemas de produção é praticamente tão importante quanto a de failover. A menos que seja cuidadosamente planejado, é pouco provável que o data center de backup tenha a mesma capacidade e desempenho que o local de produção.

Sem um plano de failback, você pode fazer um failover inicial bem sucedido e depois começar a sentir as consequências desagradáveis quando sua empresa estiver funcionando há semanas usando um local de backup que não foi aprovisionado de acordo com a demanda de produção.

Como entender os riscos

Com exceção do e-mail, é praticamente impossível saber quais aplicativos apresentam o maior risco para os negócios no caso de uma paralisação sem obter informações dos seus usuários. O RPO e RTO oferecem métricas para avaliar esses riscos. Eles também indicam quais aplicativos são prioridade nos esforços de recuperação de desastres.

Tanto o RPO como o RTO operam em conjunto. Imagine uma linha do tempo com o evento de paralisação em seu centro. O ponto do RPO está antes do evento de paralisação e indica o volume de perda de dados que um aplicativo é capaz de aguentar. À medida que o ponto se afasta do evento de paralisação, o volume de dados perdidos aumenta, e também o custo potencial para a empresa.

O RTO fica do lado oposto do evento de paralisação na linha do tempo. Ele mostra quanto tempo de inatividade o aplicativo consegue suportar até que os negócios sejam afetados. Em outras palavras, ele representa a rapidez com que você precisa se recuperar após uma pane.

Se for possível recriar as informações do sistema a partir de outras fontes, a perda de alguns dados por causa de um desastre vai dar uma certa dor de cabeça, mas não será uma catástrofe. Por exemplo, as faturas perdidas do sistema de contas a pagar podem ser recriadas pedindo que os fornecedores reenviem as solicitações de pagamento. Mas se não for possível gerar novamente os dados, como no caso de pedidos de clientes, isso poderá afetar diretamente a receita, a produtividade do usuário, a reputação da empresa, a marca em si e até a conformidade com as regulamentações.

Da mesma forma, os sistemas que não são críticos, como os relatórios mensais de um aplicativo de análise de negócios, não têm o mesmo impacto na empresa do que os sistemas envolvidos nas operações diárias, como é o caso do aplicativo de ponto de venda (POS). O RTO avalia o impacto da paralisação de um aplicativo na empresa e pode ajudar a determinar quais ferramentas de recuperação de desastres devem ser utilizadas com esse aplicativo. Os backups periódicos são uma boa opção para o aplicativo de análise de negócios, mas como o sistema POS é mais crítico para a empresa, exigirá uma solução de alta disponibilidade.

A diferença entre as métricas de RPO e RTO e os resultados reais dos testes de recuperação de desastres mostra se há uma lacuna na disponibilidade dos aplicativos. É bom lembrar que uma lacuna na disponibilidade nem sempre é indicativo do uso de uma abordagem equivocada com relação à continuidade dos negócios. As empresas normalmente têm uma grande variedade de tecnologias de recuperação de desastres de diferentes fabricantes, várias delas com muitos recursos em comum e que complicam o processo recuperação. Os testes podem ajudar a acabar com os problemas e as inconsistências nas tecnologias existentes de continuidade dos negócios e identificar áreas onde a consolidação em um único enfoque ou fabricante pode melhorar o RTO.

O que é uma boa solução de HA?

Não há segredo algum: uma solução que não dê margem para indisponibilidade dos aplicativos e perda de dados. Mas isso também vale para as pequenas e médias empresas?

A tecnologia de HA não têm mais aquele enfoque complexo e esotérico com relação à continuidade dos negócios. Há anos as grandes empresas tem usado técnicas de alta disponibilidade para proteger seus aplicativos mais críticos. A tecnologia já foi bastante testada e é amplamente aceita como padrão em ferramentas para evitar desastres. É simples, mensurável, automatizada e pode ser repetida. Tecnologias como Proteção Contínua dos Dados, replicação, e failover e failback automatizados são fundamentais.

A maturidade dos produtos de HA deixou o preço acessível para as pequenas e médias empresas. Isso, aliado à redução dos custos da infraestrutura (banda larga, virtualização de servidores, vários provedores de serviços) e à melhor usabilidade, está fazendo da HA uma alternativa muito real de continuidade para empresas de todos os tamanhos.

Inatividade e perda de dados são situações reais para empresas que dependem de TI. Amenizar esses riscos e até evitá-los com a tecnologia certa deve ser algo a ser considerado logo nos estágios iniciais do desenvolvimento de software e da implementação de produtos. Conhecendo os níveis de proteção exigidos por cada aplicativo é possível alocar os recursos apropriados. No momento em que um aplicativo estiver em uso pelos usuários, seu RPO e RTO já deverão ter sido identificados e as soluções de continuidade dos negócios implementadas para oferecer a recuperação garantida no caso de alguma pane.

Qualquer estratégia de continuidade dos negócios que não seja capaz de eliminar a inatividade e a perda de dados não tem alta disponibilidade. Há uma grande de variedade de soluções que prometem melhorar a recuperação de desastres, mas se elas não eliminarem a sua exposição, não têm alta disponibilidade.

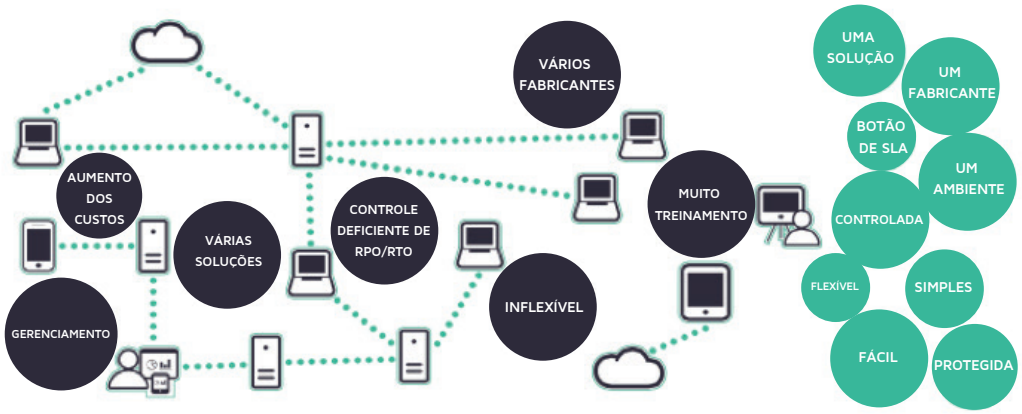

Figura 3 – Uma solução unificada para continuidade dos negócios.

Sobre a Solução Arcserve® Unified Data Protection

Há mais de 20 anos a Arcserve oferece proteção contra a inatividade para empresas em todo o mundo. Agora, a solução Arcserve® Unified Data Protection (UDP) traz um produto abrangente para todas as suas necessidades de proteção de dados e alta disponibilidade. Com controle centralizado, o Arcserve® UDP unifica backup, instantâneos, replicação e desduplicação para os seus ativos de aplicativos virtuais, físicos, dentro da empresa e na nuvem. O recurso Assured Recovery™ da solução Arcserve® UDP oferece um processo de teste abrangente e em tempo real de prontidão para um eventual desastre, para validação dos seus planos de continuidade dos negócios, sem interferir nas atividades da empresa. Para saber mais sobre a solução Arcserve® Unified Data Protection (UDP) e testar o produto gratuitamente por 30 dias, acesse http://www.arcserve.com/br/backup-disaster-recovery-it-professionals/arcserve-udp-capabilities/high-availability.aspx

Para obter mais informações sobre o Arcserve UDP, **acesse arcserve.com**