1.Continuidade da segurança da informação

A cada ano, empresas ao redor do mundo são atingidas por desastres que têm grande impacto na disponibilidade de seus sistemas. Apenas uma pequena parcela dessas empresas está adequadamente preparada para essas eventualidades. A maioria das empresas afetadas por tais enormes desastres provavelmente não sobrevive a eles. As empresas que sobrevivem a esse tipo de desastre tipicamente pensam com cuidado na possibilidade de tais desastres e, de forma antecipada, nos prováveis resultados e documentam e seguem medidas e procedimentos necessários para se proteger. No entanto, se não existirem planos, não significa que a empresa não poderá sobreviver. Isso depende do negócio e de outros fatores.

Uma organização depende de ativos, pessoal e tarefas que têm que ser conduzidas diariamente, a fim de se manter saudável e lucrativa. A maioria das organizações possui uma complexa rede de fornecedores e ativos que dependem uns dos outros para poder funcionar.

Existem canais de comunicação, tais como telefones e conexões de rede, e há edificações em que o trabalho é conduzido. As edificações devem estar em condições ótimas a fim de garantir que o trabalho não seja apenas prazeroso, mas também realizado de forma eficiente.

Se um elo na cadeia de dependências falhar, pode haver problemas. Quanto mais elos falharem, maior será o problema. E quanto mais tempo certos componentes da cadeia ficarem fora de ação, maior será o efeito disso na organização, e mais tempo levará para as operações normais reiniciarem. Pensar de forma antecipada sobre a continuidade dos processos do trabalho é essencial para uma organização.

Não importa se é um processo de produção complexo ou uma atividade relativamente simples, tal como o processamento de moradores que se mudaram para uma nova casa. Tanto para os funcionários quanto para os clientes, é importante que cada componente (grande ou pequeno) do processo trabalhe suavemente e continue a agir assim no caso de dificuldades. O propósito da gestão de continuidade de negócios (BCM) é prevenir que as atividades da empresa sejam interrompidas, proteger processos críticos das consequências de grandes perturbações nos sistemas de informação e permitir uma rápida recuperação.

Na gestão da continuidade dos processos da empresa, devem ser identificados os processos da empresa que são críticos para a operação da organização. Além de outras medidas que garantem a continuidade, deve-se evitar a perda de informações que possam ocorrer como resultado de desastre natural, ataque, incêndio ou falha de energia. As consequências dos desastres e dos incidentes de segurança e as falhas dos serviços são avaliadas em uma Análise de Impacto no Negócio (BIA). O plano da continuidade é normalmente dividido em dois componentes separados, mas intimamente relacionados. Na segurança da informação, a gestão da continuidade é normalmente dividida em dois componentes separados, mas intimamente relacionados:

- Planejamento de Continuidade do Negócio (BCP)
- Planejamento de Recuperação de Desastres (DRP)

1.1 Continuidade

A continuidade diz respeito à disponibilidade dos sistemas de informação no momento em que eles são necessários. Diversos requisitos podem ser impostos a essa disponibilidade. Dependendo da organização, do campo de trabalho e até mesmo da divisão dentro de uma organização, os requisitos de disponibilidade podem diferir dramaticamente.

1.2 O que são desastres ?

À primeira vista, um desastre parece ameaçador. Mas isso está longe de ser verdade. O fracasso de um simples sistema já poderia ser considerado um desastre. Um desastre não precisa ser necessariamente uma inundação ou um ataque terrorista. A falha do sistema de que você tanto depende para o seu trabalho diário, por meio de um problema técnico, também é um desastre.

1.3 Como a sua empresa responde a um desastre ?

As consequências que um desastre pode ter em um negócio dependem da natureza do desastre. Se o trabalho tiver sido interrompido devido a uma falha de um sistema ou de toda a rede em que a TI do escritório opera, então um telefonema para a central de serviços ou central de atendimento normalmente é suficiente para ter as atividades necessárias restauradas e funcionando. De forma similar, se a saúde de um funcionário estiver em perigo, então uma chamada telefônica para o serviço de emergência interno ou um número de emergência nacional seria a ação correta.

Em todos os casos, a vida humana tem prioridade sobre softwares e equipamentos. Atividades de evacuação devem ser postas em prática primeiro, e apenas depois deve ser dada atenção aos processos de negócios, começando pelo mais crucial. É importante, portanto, que existam procedimentos claros e eficazes definindo quais ações devem ser tomadas, por exemplo:

- Você saber que, no caso de uma falha no sistema de informação, deve contatar a central de atendimento
- Você saber onde estão as saídas de emergência em um prédio
- Você saber a quem ligar no caso de um incêndio, do acionamento espontâneo do sistema de sprinklers ou de um alerta de bomba

A central de atendimento ou o funcionário do serviço de emergência interno deve saber o que fazer em cada tipo de alerta. Os funcionários da central de atendimento terão uma lista de prioridades que documente quem é o que deve ser ajudado e quando, bem como quais organizações eles devem contatar em cada diferente alerta. A formação do pessoal do serviço de emergência interno é muito importante. Trabalhadores do serviço de emergência interno são funcionários normais que decidiram assumir essas funções adicionais. Certifique-se de que haja pessoal do serviço de emergência interno por toda a organização. Um alerta de bomba é

obviamente um risco muito sério para uma organização. Isso não é uma ocorrência normal na maioria dos países, mas se ocorrer é um desastre e pessoas podem ser mortas. É bom ver que as pessoas se tornaram mais conscientes sobre pacotes suspeitos. Itens suspeitos podem entrar em qualquer empresa. O staff deve saber o que não é normal e ser capaz de identificar itens suspeitos. Deve-se prestar atenção a isso durante a campanha de conscientização sobre segurança.

2.Plano de recuperação de desastres

A diferença entre BCP e DRP é que o DRP quer minimizar as consequências de um desastre e tomar as medidas necessárias para garantir que funcionários, ativos e processos do negócio estejam disponíveis novamente dentro de um tempo aceitável. Isso é diferente do BCP, onde métodos e procedimentos também são organizados para falhas que duram um período de tempo mais longo.

Um DRP visa uma recuperação imediata após um desastre. O DRP é posto em ação quando o desastre ainda está em curso. O trabalho é focado em determinar os danos e fazer os sistemas funcionarem novamente. Um BCP vai além e tem um foco mais amplo. O BCP planeja um local alternativo onde o trabalho pode ser realizado enquanto o local original é reconstruído. No BCP, tudo é focado em manter a empresa funcionando, mesmo que apenas parcialmente, a partir do momento em que o desastre ocorre até quando a empresa estiver totalmente recuperada.

Em outras palavras:

- **DRP:** Há um desastre agora e o que devo fazer para voltar a produção
- **BCP:** Tivemos um desastre e o que devo fazer para voltar a como era antes

Ao desenvolver um BCP e/ou um DRP, diversas soluções podem ser consideradas para ter os processos de negócio funcionando novamente. Se for decidido que, no caso de um desastre, os processos e os sistemas de negócio devem estar disponíveis o mais rapidamente possível, a melhor opção é desenvolver planos e procedimentos para um sistema de prontidão. Tais sistemas devem ser testados regularmente.

O plano também precisa incluir como o sistema de prontidão, uma vez ativado, será desativado. Deve estar claro em quais condições as operações normais podem ser retomadas. É necessário estimar o tempo máximo de inatividade e de recuperação permitidos para os sistemas e determinar quais sistemas são necessários para a organização continuar os negócios.

3.Testando o BCP

Essas diversas soluções, variando de baratas a caras, parecem todas eficazes. Um bom time de BCP/DRP considerará todas as eventualidades, discutirá tudo diversas vezes e eventualmente ganhará a aprovação da gerência superior. O plano é então publicado e todos os gerentes recebem uma cópia. Mas então as cópias vão para um armário ou gaveta. A probabilidade extremamente pequena do plano ser necessário

é a principal razão pela qual temos que estar particularmente preparados. Se o staff não tiver sido treinado e o desastre se tornar realidade, então é altamente improvável que um BCP funcione como pretendido. Testes regulares são necessários para tornar a equipe ciente de como agir no caso de um desastre. Em segundo lugar, toda a mudança que é feita ao processo de negócio deve ser incluída no plano. Um plano desatualizado não ajudará a organização a ficar operacional novamente. É possível testar o mais extensivamente possível, desde ouvir o alarme de incêndio até iniciar um hotsite ou restaurar um backup. O essencial em todos esses testes, no entanto, é que os procedimentos sejam testados em uma simulação da vida real, a fim de ver se essas medidas são corretas e eficazes.

4.Redundâncias

4.1 Local redundante

Uma boa alternativa para um negócio com muitas localidades, mas apenas um único centro de computação, é um local redundante. O local redundante contém uma cópia do centro de computação. Todos os dados que entram no centro de computação principal também são inseridos no sistema do local redundante. Se um desses dois locais sofrer uma falha, o outro local assumirá automaticamente.

4.2 Hotsite sob demanda

Outra solução é um hotsite móvel. Trata-se de um ou mais caminhões que contêm todo o equipamento necessário para funcionar como um centro de computação temporário. No caso de um desastre, os caminhões são conduzidos em um curto período de tempo, tipicamente de algumas horas, para uma localização predefinida e o equipamento é conectado. As possibilidades são limitadas, mas é uma forma de ter os processos mais cruciais operacionais novamente, o mais cedo possível.

4.3 Locais de trabalho alternativos

Certas pessoas-chave da organização foram designadas para locais de trabalho alternativos em outras filiais. Se algo acontecesse no local de trabalho permanente dessas pessoas-chave, eles(as) viajariam alguns quilômetros para o local de trabalho alternativo. O funcionário que trabalha nesse local alternativo está ciente do arranjo e abrirá espaço para essa pessoa-chave, se necessário.

4.4 Medidas para o staff

Um desastre pode resultar em problemas de staff se as pessoas que apoiam o processo principal também estiverem diretamente envolvidas no desastre e, como consequência, não estiverem mais disponíveis. Os planos devem incluir formas de substituir essas pessoas-chave. No caso de um grande problema que afete a localidade, em vez de apenas a empresa, as pessoas podem ser incapacitadas de viajar, especialmente para um local remoto.