Política de backup dos colaboradores.

Explicar os principais conceitos relacionados ao assunto backup e a importância dele dentro do processo de segurança da informação, além de descrever como um programa identifica que um determinado arquivo necessita ou não passar pelo processo de backup.

Como vimos nas aulas anteriores, a análise de risco é um processo que identifica sistematicamente os recursos que são valiosos para a empresa, bem como identifica as ameaças que podem explorar as vulnerabilidades dos ativos de informação. Dessa maneira, é possível quantificar as possíveis perdas relacionadas a eventos de insegurança, além de poder recomendar a melhor forma para que se faça a alocação dos recursos financeiros necessários para implementar a proteção.

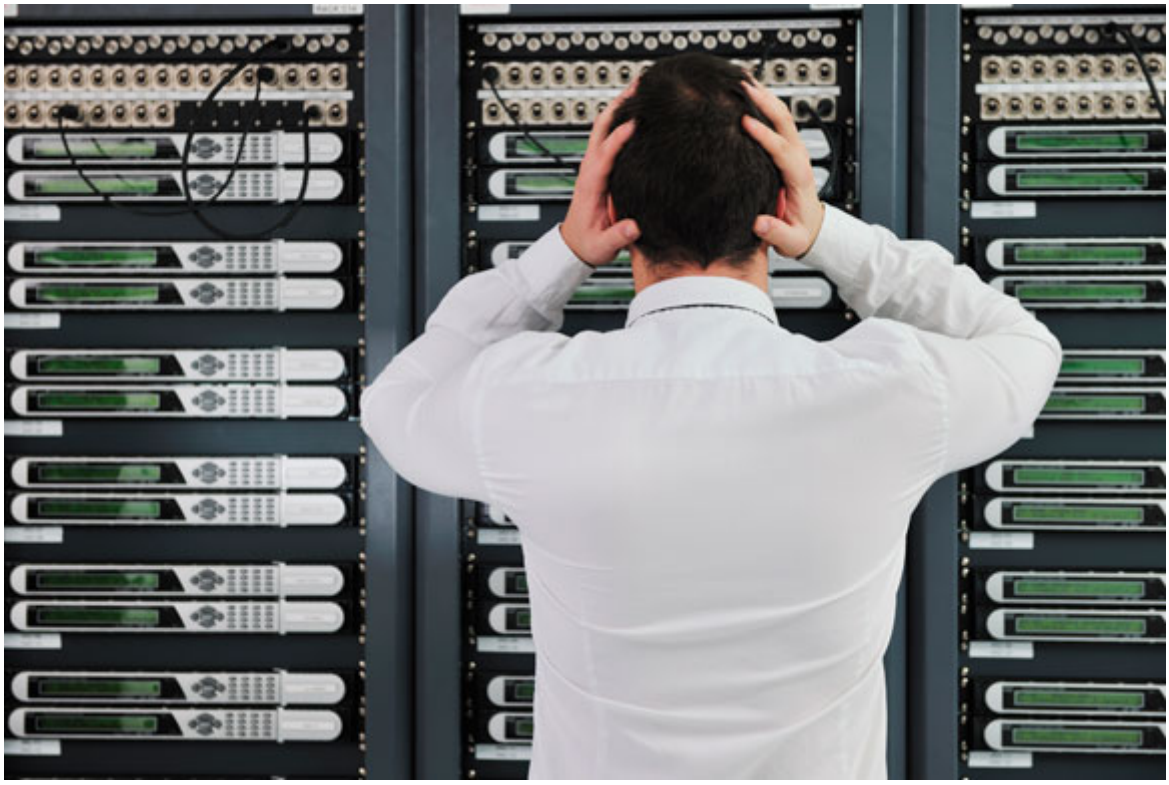
O risco tem duas importantes características, que são a gravidade/dano e a probabilidade da ocorrência, sendo a gravidade definida como o pior acidente que possa ocorrer, e a probabilidade a possibilidade de algo ocorrer mediante os cenários existentes.

Backup

Antes de iniciar este módulo, é importante conceituar a palavra backup como sendo um tipo de cópia de segurança que é realizada por parte das pessoas com a intenção de poder recuperar algum dado ou informação, quando for necessário**.**

A maioria das pessoas só percebe a importância do backup quando ocorre algum incidente de segurança e é necessária a recuperação dos dados que, muitas vezes, podem ser de fundamental importância para a sobrevivência de uma empresa.

Às vezes, mesmo tendo um backup, ele pode não ser suficiente, pois não foi feito da forma correta e as fases de planejamento, levantamento da informação, criticidade dos dados, classificação da informação, entre outras foram deixadas de lado e, com isso, não se conseguiu verificar qual era a real necessidade da empresa e quais deveriam ser as informações que deveriam estar protegidas pelo processo de backup.



Como vimos anteriormente, a área de informática ficou sendo a custodiante da informação e, por isso, tem uma série de responsabilidades a serem feitas de forma a manter a disponibilidade, integridade dos dados, e uma dessas atividades está diretamente relacionada ao processo de backup.

Muitas vezes, é criado um procedimento de backup de forma incorreta, não por negligência, mas por falta do conhecimento de conceitos relacionados ao assunto. Existem várias modalidades e tipos de backup que podem ser realizados dentro do ambiente de tecnologia da informação e que muitas vezes são tratadas ao pé da letra e acabam não atingindo o objetivo esperado. Desse modo, antes de continuar com este assunto, faz-se necessário entender alguns conceitos relacionados ao Backup.

Uma dúvida comum relacionada ao backup, e que, a partir do momento em que conseguimos

esclarecê-la, passamos a entender como funciona o processo de backup como um todo está relacionada ao fato de não conseguir entender como o programa de backup identifica que o arquivo necessita ser backupeado ou não.

O processo é bem simples, a maioria dos programas de backup utiliza algum atributo do arquivo para verificar se ele necessita ser backupeado ou não. No nosso exemplo, vamos supor que exista um atributo chamado ponteiro. Se esse ponteiro estiver marcado, é sinal de que esse arquivo nunca foi backupeado, ou foi alterado recentemente depois da última vez que ele passou por algum tipo de backup. Em contrapartida, se esse atributo está desmarcado, é sinal de que esse arquivo já foi copiado pela ferramenta de backup (é claro que essa informação só será válida dependendo do tipo de backup rodado – full e incremental neste caso, pois são os únicos que mexem no atributo do arquivo).

Assim, quando criamos um arquivo dentro de um diretório qualquer do nosso HD, ou quando copiamos algum arquivo para dentro de um diretório qualquer ou até mesmo quando fazemos alguma alteração em algum arquivo, o atributo é **marcado**.

Política de backup

Podemos definir como politica de backup o conjunto de atividades que deverão ser realizadas para poder salvaguardar os dados da empresa e possibilitar a continuidade dos seus negócios após um incidente de segurança. A politica de backup abordará aspectos que envolverão diversos itens como: "tecnologia a ser implementada (hardware/softwares), volume de dados, periodicidade dos backups (mensal, semanal, quinzenal, anual), vida útil da informação dentro do processo de backup, (a data do backup mais antigo), interferência no ambiente de produção (janelas de backups), responsáveis pelo processo de backup, procedimentos operacionais (indicando como, onde, quando e quem faz o backup), armazenamento das mídias, tipos de mídias (LTO, DLT, DAT, AIT, CD, DVD, NAS (Network Arry Storage), custos iniciais e finais, necessidade de replicação ou não de informações, geração de imagens dos sistemas, necessidades de agentes (programas especiais que

fazem conexões com dados de correio eletrônico, banco de dados de uma forma segura, pois essas aplicações são proprietárias, testes e restauração, cópia de arquivos abertos (Open File), dentre outros que não envolvem a tecnologia, como a conscientização dos usuários para que armazenem os dados nos locais corretos e que estarão cobertos pela política de backup".

Tipos de backups

O mercado trabalha com cinco tipos de backups, que serão descritos a seguir (diário, full, incremental, cópia e diferencial).

- **Backup diário** – como o próprio nome diz, esse tipo de backup, ao ser executado, verifica dentre os arquivos que foram selecionados para fazer o backup, aquele que possui a sua data igual a do dia que será rodado o backup. Caso exista algum arquivo, dentre os selecionados, que não tenha sido criado ou alterado no mesmo dia que foi executada a tarefa de backup, o processo de backup ignora o arquivo. Esse tipo de backup tem outra característica que é de não se preocupar se o arquivo já foi backupeado alguma vez ou não. Para o processo, a única coisa que interessa é a data de criação/alteração do arquivo. Dessa forma, ao terminar a execução do backup, o atributo do arquivo ficará igual ao estado que estava antes da execução do backup.Geralmente realizamos esse tipo de backup quando não desejamos interferir na politica de backup estabelecida pela empresa. Podemos fazer esse tipo de backup várias vezes ao dia. Pelo fato de não alterar/modificar o atributo do arquivo, quando esse backup é executado pela segunda vez em cima do mesmo arquivo, mesmo que não tenha ocorrido nenhuma alteração nele, o arquivo é novamente copiado.
- **Backup cópia** – imagine que você selecionou uma quantidade X de arquivos para serem copiados. Quando for executado o backup do tipo cópia, ele fará exatamente uma cópia fiel de todos os arquivos que foram selecionados, independentemente da data de criação ou do atributo do arquivo, pois para ele só interessa criar uma imagem de todos os arquivos selecionados, sem pensar em alterar o atributo do arquivo. Esse tipo de backup, como o anterior também, pode ser realizado diversas vezes durante o dia, porém com a pequena diferença de que ele copiará tudo o que estiver selecionado e mesmo que o arquivo já tenha sido gravado anteriormente. Pelo fato de não alterar/modificar o status do atributo do arquivo, esse tipo de backup também não interfere nas políticas de backups da empresa e pode ser feito a qualquer momento (respeitando-se o volume de dados e interferência na rede de dados da empresa).

- **Backup full ou normal** – esse é o tipo de backup que deve ser feito no inicio do processo da política de backup, pois ele tem como característica copiar todos os arquivos que estiverem selecionados, independentemente de ter o atributo do arquivo marcado ou não, e, ao final da sua tarefa, desmarcar todos os arquivos que estiverem com o atributo marcado. Para esse tipo de backup não interessa se o arquivo já foi copiado ou não, a única coisa que realmente importa é que, ao final da cópia, nenhum arquivo que passou pelo processo pode continuar com o atributo marcado.
  Em consequência dessa característica, esse tipo de backup não deve ser feito a qualquer momento, pois ele acaba por interferir na rotina de backup estabelecida pela empresa, uma vez que altera os atributos dos arquivos.
- **Backup incremental** – nesse tipo de backup a ideia é copiar apenas os arquivos que foram criados ou alterados e que não tenha sido backupeados ainda, ou seja, tenham o seu atributo de arquivo marcado. Caso o arquivo não possua o atributo marcado, o processo de backup vai ignorar os arquivos e não copiará nada. Caso o arquivo esteja com o atributo marcado, após a cópia do arquivo ele desmarcará o atributo do arquivo. Dessa maneira, se logo em seguida for solicitado

rodar o backup incremental desses mesmos arquivos novamente e não houver ocorrido nenhuma alteração neles, nada será copiado.

- **Backup diferencial** – da mesma forma que o backup do tipo incremental, esse tipo de backup apenas copiará os arquivos que foram criados ou alterados, ou seja, estejam com o seu atributo de arquivo marcado. Caso o arquivo não esteja com o atributo marcado, o processo de backup vai ignorar os arquivos e não copiará nada. A única diferença é que, após a cópia dos arquivos, ele não mexerá nos atributos dos arquivos. Assim, se após terminar o backup diferencial, rodar novamente um backup desse mesmo tipo, ele vai copiar os mesmos arquivos que foram copiados anteriormente, ou seja, os mesmos arquivos que estavam marcados.

Quando falamos em estratégias de backup, o administrador da rede poderá combinar os tipos de backup da melhor forma possível, e dependendo da escolha, haverá maior ou menor utilização da fita. Como exemplo podemos citar uma estratégia em que serão realizados backups todos os dias, de domingo a sábado, e aos domingos serão realizados backups do tipo full, e de segunda a sábado serão rodados backups do tipo incremental, utilizando para isso uma fita para cada dia. Esse tipo de estratégia permitirá a execução de backups em um período de tempo pequeno, uma vez que apenas no backup que é realizado no domingo haverá uma demora, pois todos os arquivos deverão ser copiados. Nos demais dias da semana serão apenas copiados os arquivos que foram criados ou alterados depois da execução do backup full. Se por acaso ocorrer um problema no HD desse servidor, por exemplo, na sexta-feira, basta apenas recuperar o backup full que foi feito no domingo e depois todas as fitas que possuem o backup incremental até quinta-feira que teremos novamente o servidor com a posição anterior ao dia da falha. Nesse tipo de estratégia, caso alguma fita incremental apresente defeito, o backup desse dia estará comprometido, já que na fita do dia posterior os arquivos não estarão copiados, pois o seus atributos foram apagados após a realização do backup incremental anterior.

Outra estratégia seria fazer também backups de domingo a sábado, e no domingo executaria o backup do tipo full, e, de segunda a sábado, executaria os backups do tipo diferencial. Esse tipo de estratégia teria o tempo de execução da atividade no seu início parecido com a outra estratégia, porém na medida em que os dias da semana fossem passando, pelo fato desse tipo de backup não desmarcar os atributos dos arquivos, aumentaria a quantidade de arquivos que seriam copiados no dia e na respectiva fita. Se ocorrer o problema que ocorreu na situação exposta anteriormente, porém, bastaria apenas restaurar o backup do domingo e depois a fita de quinta-feira, que teríamos o servidor novamente recuperado com a posição de um dia antes da falha. Apesar de demorar mais na confecção e gastar mais espaço na fita, esse tipo de estratégia permite recuperar o servidor com menos troca de fita, além de que, se ocorrer algum problema com alguma fita, o arquivo poderá ser novamente gravado pelo processo do dia anterior, uma vez que o seu atributo não será apagado. O único problema pode acontecer caso a pessoa apague intencionalmente esse arquivo e, desse modo, mesmo que rode novamente o backup diferencial, os arquivos não poderão ser copiados.

Em uma politica de backup, diversos aspectos também deverão ser considerados, como os detalhados a seguir.

O que se pensar antes de montar a política de backup?

O que copiar?

Essa pode ser a primeira dúvida que o administrador de rede terá quando tiver que criar a sua política de backup. É claro que, se as atividades anteriores como análise de risco e classificação da informação já tiverem sido realizadas, isso o ajudará muito na tomada de sua decisão, porém, caso essas atividades não tenham sido realizadas, a resposta às perguntas como:

- Qual é a utilidade da informação para a empresa?
- Essa informação tem algum valor para a empresa?
- Qual é o período de validade da informação?
- Será que esta informação tem algum valor para a empresa?
- Sua perda pode trazer algum impacto para a empresa?
- A empresa consegue viver sem esta informação?
- Se a direção da empresa necessitar desta informação e eu não a tiver, o que acontece?

Tipo de software a ser utilizado

A escolha de um software de backup é de extrema importância para a política de backup, uma vez que alguns softwares nativos dos sistemas operacionais oferecem apenas recursos básicos e que podem não ser suficientes para proteger os dados da maneira adequada, pois dependendo da situação, o software de backup nativo do sistema operacional não terá direito a acessar dados de serviços que estiverem instalados nos servidores e que tenham características de ser proprietário, ou seja, somente a própria aplicação pode ter acesso aos dados.

Um exemplo de uma situação como essa pode ser visto com relação ao banco de dados SQL, que não permite que o sistema operacional faça a cópia da sua base. Nesse caso, apenas o próprio SQL teria direito de fazer a cópia desses dados.

Em soluções de softwares de backup específicas, existe a possibilidade de a ferramenta conseguir fazer esse backup, e, nesse caso, são instalados agentes que permitem à ferramenta acessar o banco de dados e fazer a cópia de segurança necessária.

Além disso, outros itens também relacionados à escolha do software de Backup, por exemplo: o software permite programar backups de forma automática? Ele copia arquivos abertos? Os softwares são amigáveis e fáceis de utilizar? O software permite utilizar variada solução de dispositivos de backup e fitas? Permite guardar histórico das atividades realizadas? É compatível com vários tipos de sistemas.

A ideia aqui não é esgotar o assunto, apenas procurar mostrar a complexidade com a qual o administrador estará envolvido.

Volume de dados a serem copiados

Dependendo do volume de dados que deverá ser copiado, a estratégia de backup também sofrerá uma interferência muito grande, pois novas variáveis como tempo e capacidade de fita deverão ser combinadas para que se possa adotar a melhor estratégia. Dependendo da quantidade, pode-se decidir fazer backups em HD´s, Storages, NAS ou SAN, em vez de fazer backup em fitas.

Também pode-se fazer backup em bibliotecas robôs (LIB´s), que permitem fazer o backup com um conjunto maior de fitas e agrupadas dentro de um mesmo equipamento.

A janela do backup

É o tempo que se demora em completar uma operação de backup, além de estar relacionada ao tempo que um sistema ficará dedicado exclusivamente à operação de backup sem que haja gravação dos dados na mídia que está sofrendo o backup. Explicando melhor, a janela de backup representará o tempo disponível que temos para executar o processo de backup em um determinado volume de dados. A determinação da janela pode estar associada ao ciclo de atualização de dados de uma determinada aplicação.

Observações importantes

Não adianta ter um processo de backup todo estruturado se não são feitos restores para verificar se os dados que foram gravados nas mídias magnéticas podem ser recuperados quando forem requisitados em uma situação de emergência.

As mídias magnéticas, se ficarem armazenadas no mesmo local em que estão os servidores, podem colocar todo o processo em risco, uma vez que se houver indisponibilidade do local, tanto os servidores como as informações de recuperação estarão inacessíveis.

Devemos levar em consideração que as mídias magnéticas e equipamentos de backups podem apresentar defeitos e falhas e, por isso, a duplicação de dispositivos deve ser pensada para aumentar a disponibilidade.

Para facilitar o gerenciamento e a execução do processo de backup, é importante que os dados e as informações dos colaboradores da organização fiquem centralizados dentro dos servidores de arquivos, em vez de ficarem distribuídos dentro das suas estações de trabalho.

Para conhecer um pouco mais sobre essas atividades, veja a animação a seguir. A animação faz parte da sequência desta aula e, portanto, é essencial para a aprendizagem.

objeto disponível apenas na versão web

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento. Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

objeto disponível apenas na versão web

objeto disponível apenas na versão web

Referências

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de segurança da informação: guia prático para elaboração e implementação.* Rio de Janeiro: Ciência Moderna, 2006.

FIALHO JUNIOR, Mozart. *Guia essencial do backup.* São Paulo: Digerati Books, 2007.

SOUZA, Lindeberg Barros. *Redes de computadores: dados, voz e imagem.* 2.ed. São Paulo: Erica, 2000.

WADLOW, Thomaz A. *Segurança de redes em ambientes: projeto e gerenciamento de redes seguras*. Rio de Janeiro: Campus, 2000.