Introdução a Segurança da Informação – Parte 1

13 de abril de 2015 / maximoz

Políticas de segurança e procedimentos

As políticas de segurança protegem sua companhia contra ameaças externas ou internas aos dados importantes. Se você criar políticas de senhas, instalar Firewall, limitar o acesso aos dados mas esquecer de criar políticas de segurança e definir um procedimento para implementá-las, você está trancando todas as suas portas mas deixando uma janela aberta. Todas as suas medidas de segurança são inúteis se você não definiu uma boa prática de segurança para proteger os dados da sua companhia.

Uma política de segurança da informação é um conjunto de regras e práticas que definem como as informações sensíveis de uma companhia devem ser gerenciadas, protegidas, e distribuídas dentro da empresa. Os diferentes aspectos de uma política de segurança da informação incluem rotular as informações, as modificações das informações, a responsabilidade e a informação proprietária.

Cada companhia tem uma estrutura de organização, e os funcionários em diferentes níveis acessam diferentes tipos de dados. A classificação das informações e a distribuição das políticas de dados são, portanto, importantes para uma companhia, então aqueles funcionários de níveis inferiores não devem ser permitidos acessar dados armazenados para os funcionários de níveis superiores.

Além disso, todo tipo de informação que uma companhia armazena não é igual e, portanto, não requerem o mesmo nível de proteção. Por isso, a classificação de segurança da informação, bem como a identificação do gestor de alto nível como proprietário da informação são importantes.

É importante lembrar que para cada tipo de informação, uma companhia precisa desenvolver políticas sobre quais informações estão disponíveis e para qual propósito ela irá ser disseminada. Os principais objetivos da política de segurança da informação são:

1. **Confidencialidade** – propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
2. **Integridade** – propriedade que garante que a informação manipulada mantenha todas as suas características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).
3. **Disponibilidade** – propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.
4. **Autenticidade** – propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

Outra parte importante de uma política de segurança é definir a autoridade e a delegação da autoridade para as políticas. Um sistema pode definir quatro tipos de usuários envolvidos em processos de segurança. Desses tipos, são eles:

Uma política deve definir os papéis e responsabilidades de cada tipo de função de usuário envolvido nos processos de segurança. Se o sistema de segurança suporta grupos então a política deve definir se um usuário pode pertencer a mais de um grupo, como resolver conflitos entre as exigências de prestação de contas individuais dentro um grupo, usuários individuais e privilégios de grupo.

Próximo capítulo >>>

Traduzido e adaptado por: Maximoz Sec
Artigo original: http://learnthat.com/introduction-to-network-security/

, ,