Introdução a Segurança da Informação – Parte 3

13 de abril de 2015 / maximoz

Processos de segurança da informação

O processo de segurança da informação é o método que uma companhia usa para implementar segurança na organização. Este inclui elementos como:

1. **Avaliação de Risco:** Inclui a identificação de ameaças e vulnerabilidades do sistema e avaliação dos riscos associados à eles e a probabilidades de suas ocorrências.
2. **Estratégia:** Diz respeito ao plano de mitigar o risco que está associado às políticas de segurança, procedimentos e treinamento. O plano deve ser revisado e aprovado pelo conselho de administração.
3. **Autorização:** A atribuição de funções e responsabilidades aos usuários envolvidos nos processos de segurança.
4. **Monitoramento de Segurança:** Está relacionado ao uso de diversos métodos que serão usados para assegurar que os controles de segurança são efizaces e executam as tarefas pretendidas como desejado. Além dele, inclui a garantia de que o risco está devidamente avaliado e mitigado.

Implementação de política de segurança

Uma vez que a política de segurança é definida e aprovada, o plano de implementação da política deve ser posto em ação. Geralmente é fácil criar uma política, mas muito difícil implementá-la. A medida para implementar a política de segurança é educar os membros da equipe acerca da política e exigências de segurança da companhia.

Para implementar segurança em uma companhia é importante que não somente os funcionários mas a gestão sênior e o conselho de administração também participem em processos de segurança. A atitude da gestão sênior afeta o compromisso de toda a companhia para a segurança. Pessoas externas associadas com a companhia como empreiteiros e auditores devem também apoiar os processos de segurança.

O conselho de administração deve claramente especificar suas expectativas de segurança à gestão e aprovar planos, políticas e programas de segurança. Um relatório anual – ou periódico – deve ser feito sobre a eficácia dos programas de segurança da informação.

Os oficiais de segurança, por outro lado, devem ter conhecimento e treinamento suficiente para manusear uma situação de crise. Eles devem também ter a autoridade para responder a um evento de segurança e terem permissão para tomar ações imediatas em tempos de emergência.

Os funcionários da companhia têm de estar conscientes da política de segurança da empresa. Além disso, eles devem conhecer suas funções e prestar contas de suas responsabilidades. Seus contratos de trabalho devem especificar cada detalhe em relação a seus afazeres gerais.

A política de segurança deve ser disponibilizada para que os funcionários possam consultá-la a qualquer momento e de maneira fácil. O programa de conscientização de segurança pode ser definidio. As linhas de comunicação amigáveis e informais devem ser abertas entre o Escritório de Segurança de Informação e os funcionários.

Os funcionários da empresas devem também estar cientes das violações de segurança para que eles saibam completamente das repercussões de violação da política de segurança. Caso contrário, isso ajudaria a exposição não intencional de informaçõe sensíveis para os atacantes ou causar violações intencionais.

As violações da política devem ser manipuladas de acordo com os termos do AUP (Uso Aceitável da Política) da política.

Próximo capítulo >>>

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