Introdução a Segurança da Informação – Parte 2

13 de abril de 2015 / maximoz

Implementação de boas medidas de segurança

A implementação de boas medidas de segurança na sua companhia podem garantir a segurança, integridade e dispobilidade dos dados. As medidas de segurança para proteger os dados da sua companhia podem ser alcançados construindo uma boa política de segurança para a companhia além de outras coisas. Uma política de segurança é o alicerce das medidas de segurança tomadas pela companhia. Ela é a primeira medida de segurança para reduzir o risco de utilização inaceitável de recursos de informação da companhia.

A política de segurança deve precisamente informar todos os empregados sobre o uso geral dos recursos da companhia, seu uso aceitável, as atividades proibidas e as responsabilidades dos funcionários relacionados com a segurança.

Ela também deve descrever o uso aceitável de todos os ativos da companhia, que incluem hardware, sotfware e internet. Se uma velha política de segurança já existe então ao invés de perder tempo criando uma nova política, é melhor reconstruir a antiga. Deve ser atualizada periodicamente de acordo com o surgimento de novas ameaças. Algumas outras medidas de segurança que devem ser tomadas pela comapnhia para implementar uma boa segurança são:

1. **Alterar Senhas:** As senhas de todos os servidores que hospedam importantes serviços devem ser mudadas frequentemente. Por exemplo, um servidor de importantes serviços hospeda contas de usuários, firewalls e roteadores. Mudança frequente nas senhas garante que um atacante não possa ganhar acesso ao sistema facilmente.
2. **Revisar Contas de Usuário e Listas de Acesso:** A avaliação regular de contas de usuário e listas de acesso permitem manter sua rede atualizada com os funcionários que acessam os recursos da rede. Muitas vezes, os funcionários que já deixaram a companhia ainda tem permissões de acesso aos recursos da companhia. Isso pode levar a quebra da segurança.
3. **Criar uma política de "Não Wireless":** O acesso de dispositivos Wireless são difíceis de proteger e monitorar. Por isso, eles devem ser desligados da rede. Dispositivos pessoais não devem ser permitidos em uma rede corporativa. Se você precisar ter ativos numa rede corporativa, você deve criar uma política para cobrir esses dispositivos, ou seja, criar uma rede Wireless somente para determinados usuários.
4. **Implementar um Sistema de Detecção de Intrusão:** O sistema de detecção de intrusão irá detectar e prevenir todos os ataques direcionados ao sistema/rede. Veremos mais sobre ele mais adiante.
5. **Criar um Plano de Resposta a Incidente:** O plano de resposta a incidente deve ser criado e o Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores (CERT) deve estar incluído nele. Isso garante que os membros da equipe ou segurança pessoal saibam quem chamar primeiro e como investigar um evento em caso de emergência ou roubo.

Próximo capítulo >>>

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