Introdução a Segurança da Informação – Parte 4

13 de abril de 2015 / maximoz

Controle de acesso

O objetivo do controle de acesso é assegurar que o acesso da informação seja restrito comente à pessoas que tenham autorização de acessar aquela informação. Para implementar o controle de acesso, é importante que você tenha políticas de segurança em vigor na sua empresa e um claro conjunto de funções e responsabilidades definidas para pessoas envolvidas na gestão de segurança.

Há um número de modelos de controles de acesso disponíveis que ajudam você a garantir que somente pessoas autorizadas possam acessar a informação. Os modelos de controle de acesso ajudam uma empresa a definir suas políticas de segurança, eles são baseados em dois princípios principais:

1. **Permissões Implícitas:** Nesse, certos usuários são bloqueados implicitamente e, sem seguida, permissão ou negação são configurados para eles. Por exemplo, os arquivos ***at.allow*** e **at.deny** configurados no UNIX permite/nega o serviço aos usuários nomeados nos arquivos.
2. **Privilégio Mínimo:** Para os usuários são atribuídos somente as permissões necessárias para que eles exerçam seus trabalhos.

Os diferentes modelos de controle de acesso são:

1. **Modelo de Bell-La-Padula (BLM):** Esse é um modelo multi-nível desenvolvido por Bell e LaPadula. Foi especialmente criado para o governo e aplicações militares para implementar o controle de acesso. É baseado no princípio do privilégio mínimo e previne os usuários de acesso a informação que tem classificação de segurança mais alta do que a que eles são autorizados. Um problema com esse modelo é que ele não consegue lidar com a integridade dos dados.
2. **Modelo Biba:** Esse modelo foi criado para remover os malefícios do modelo Bell-La-Padula. Ele toma ênfase na integridade dos dados e não permite escrever ou ler os dados. Isto é, os usuários não podem corromper os dados armazenados de posto mais alto ou obter dados corrompidos por usuários de posto mais baixo. Eles podem somente criar conteúdo igual ou inferior ao seu nível de integridade e pode visualizar o conteúdo apenas em ou acima de seu próprio nível de integridade.
3. **Madelo Clark-Wilson:** Esse modelo foca no fluxo de informação em todas as direções e não apenas acima ou abaixo como feito pelos modelos Bell-La-Padula e Biba. O Clark-Wilson impede uma operação de ocorrer se for ilegal.
4. **Modelo de "Não-interferência":** Esse assegura que as funções de segurança de alto nível não interfiram com as funções de segurança de nível mais baixo. Isso previne que o usuário de nível inferior seja afetado pelas mudanças feitas para o nível mais elevado de um sistema.

Autorização & Autenticação

Um mecanismo de controle eficaz deve também estar implementado para proteger os recursos da companhia. Os indivíduos autorizados que incluem os funcionários, fornecedores, prestadores de serviço, clientes ou visitantes devem receber permissões apropriadas para acessar dispositivos de rede autorizados de acordo com as políticas da companhia.

É importante averiguar se as pessoas e os sistemas que tentam acessar os recursos da companhia são de fato as pessoas ou sistemas que afirmam ser. Técnicas de autenticação permitem identificar e autenticar as pessoas e sistemas. Autenticação funciona em conjunto com a identificação. Uma vez que a identidade de uma pessoa é estabelecida pelo sistema, a autorização possibilita um sistema saber se o usuários tem permissão para acessar os recursos requisitados ou não.

A autenticação depende de três fatores principais que incluem fatores como: algo que você sabe – por exemplo o número de identificação pessoal (PIN) e senha, algo que você tem – por exemplo um cartão inteligente, e algo fisicamente único sobre você – por exemplo suas impressões digitais (fingerprints) ou padrões de retina.

Por vezes, a autenticação multifatorial é também usada em que dois ou mais métodos de autenticação são usados. Por exemplo, o uso de cartões inteligentes e as senhas. Alguns métodos comuns de autenticação usados nos dias de hoje são: Usuário/Senha, Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Certificados, Tokens Seguros e o Kerberos.

Próximo capítulo >>>

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