Gerência de Segurança

- Gerência de segurança envolve a proteção de dados sensíveis dos dispositivos de rede através do controle de acesso aos pontos onde tais informações se localizam

Gerência de Segurança

- Benefícios do processo de gerência de segurança
- Realizando a gerência de segurança
- Conectando-se a uma rede pública
- Gerência de segurança em um Sistema de Gerência de Redes
- Reportando eventos de segurança

Benefícios do Processo de Gerência de Segurança

- Segurança
  - Eliminar o acesso a informações sensíveis através da rede de comunicação de dados
  - Solução drástica e não prática
- Gerência de Segurança
  - Oferecimento de uma alternativa prática, para transferência e armazenamento de informações

Realizando a Gerência de Segurança

- Segurança de informações sensíveis x necessidade de acesso dos usuários
- A gerência de segurança envolve quatro passos:
  1. Identificar as informações sensíveis
  2. Encontrar os pontos de acesso
  3. Prover segurança para os pontos de acesso
  4. Manter a segurança dos pontos de acesso

Realizando a Gerência de Segurança

- Identificando as informações sensíveis
  - Definidas pela política da empresa
    - Financeiras, mercado, projetos, informações de clientes, informações de empregados, etc
  - Identificação dos computadores que guardam tais informações

Realizando a Gerência de Segurança

- Encontrando os pontos de acesso
  - Conexão física
  - Login Remoto (telnet)
  - Transferência de arquivos (ftp)
  - Correio eletrônico (email)
  - Execução remota de processos
  - Servidores de diretórios e arquivos
  - Enfim, qualquer serviço de rede é uma porta de entrada

Realizando a Gerência de Segurança

- Provendo segurança para os pontos de acesso
  - Segurança pode ser implantada em várias camadas da rede
    - Criptografia, na camada de enlace de dados
    - Filtros de pacotes, na camada de rede
    - Autenticação, na camada de aplicação

Realizando a Gerência de Segurança

- Criptografia
  - Codificação da informação
  - Indicada quando o meio é compartilhado
  - Algoritmos de chave privada
    - Mesma chave para codificação e decodificação
    - Chave deve ser trocada periodicamente
  - Algoritmos de chave pública
    - Chaves com duas partes: uma privada e outra pública
    - Exemplos:
      - DES (Data Encryption Standard)
      - SNMPv2 usa algoritmo de chave pública

Realizando a Gerência de Segurança

- Filtros de pacotes
  - Permite que pacotes passem (ou não) pelo DR, dependendo de seu endereço
  - DR deve ser configurado
  - Mudanças no endereço da fonte pode atrapalhar o funcionamento do filtro
  - Exemplos:
    - Endereço MAC de placa de rede
    - Programas que permitem alterar endereço MAC

Realizando a Gerência de Segurança

- Autenticação de computador
  - Permite o acesso a um serviço baseado no identificador do computador
    - Exemplo: xhosts +athenas
  - Informação de identificação do computador pode ser facilmente alterada

Realizando a Gerência de Segurança

- Autenticação de usuário
  - Identificação do usuário antes de permitir acesso
  - Uso de senha
    - Formato texto
    - Senhas fáceis (mnemônicas)
  - Uso de criptografia para senhas
    - Secure Shell (SSH)
  - Uso de senhas descartáveis
    - se for roubada não poderá ser usada

Realizando a Gerência de Segurança

- Autenticação de chave
  - Provê autenticação de usuário e de computador em conjunto
  - Servidor de chaves
    - Acesso remoto só pode ser feito com uma chave válida
    - Servidor autentica fonte (usuário e computador) e gera a chave para aquela transação
  - Exemplo:
    - Kerberos, MIT

Realizando a Gerência de Segurança

- Mantendo a segurança dos pontos de acesso
  - Localização de brechas atuais ou potenciais na segurança
    - Programas geradores de senhas e chaves de criptografia
    - Programas de ataques
    - Lançando desafios a hackers

Conectando-se a uma Rede Pública

- A conexão à uma rede pública muda o enfoque da gerência de segurança
- Tipos de acesso a partir de uma rede pública
  - Sem acesso
  - Acesso total
  - Acesso limitado

Conectando-se a uma Rede Pública

- Sem acesso
  - Nenhum serviço de rede disponível externamente.
  - Serviço de troca de mensagens programado
    - Vírus podem se propagar usando email
- Acesso total
  - Todos os computadores devem prover mecanismos de segurança
  - Solução perigosa

Conectando-se a uma Rede Pública

- Acesso limitado
  - Apenas um subconjunto dos computadores pode ser acessado externamente
  - Uso de firewall
    - Todos os acessos externos devem passar por um único computador
    - Mecanismos de segurança apenas neste computador
  - Limitação dos serviços de rede oferecidos
    - Exemplo: SSH ao invés de telnet

Gerência de Segurança em um SGR

- Ferramentas de gerência de segurança devem limitar o acesso e notificar o ER em caso de brechas na segurança
- Tipos de ferramenta
  - Simples
  - Mais complexa
  - Avançada

Gerência de Segurança em um SGR

- Ferramenta Simples
  - Deve exibir (graficamente) onde a segurança está implementada
  - Operar em conjunto com a gerência de configuração
  - Ferramentas disponíveis
    - Verificação de configuração
    - Inspeção manual dos mecanismos de segurança implementados

Gerência de Segurança em um SGR

- Ferramenta mais complexa
  - Monitoração em tempo real dos pontos de acesso
  - Interação com a interface gráfica para geração de avisos e alarmes
    - Tentativas de acessos não autorizados
    - Tentativas sucessivas
  - “Inteligência” para analisar o registro de eventos
  - Funcionalidades não disponíveis nas

Gerência de Segurança em um SGR

- Ferramenta Avançada
  - Análise das conseqüências das medidas de segurança
    - Restrição de tráfego
    - Desempenho dos DR

Reportando Eventos de Segurança

- Relatórios com histórico de eventos
  - Identificação de tentativas (com sucesso ou não) de acessos não autorizados
  - Identificação de eventos devido a problemas de configuração
- Aplicações de tempo real
  - Evitar acessos não autorizados
- Responsável pela segurança?