UGB
Centro Universitário Geraldo Di Biase

PROJETO DE REDES
www.projetoderedes.com.br

Auditoria e Análise de Segurança da Informação

Trilha de Auditoria

Prof. José Maurício S. Pinheiro - UGB - 2009

Um problema comum em segurança é identificar quem ou o que causou algo.

Auditoria de Segurança

Auditoria de Segurança é uma técnica de avaliação sistemática e mensurável da política de segurança de uma organização aplicada a um local específico.

Exemplo: Teste de Invasão (Penetration Test) - Enfoca-se na tentativa de encontrar falhas em recursos críticos de uma organização.

Auditoria de Segurança

- Auditorias de segurança não são ações isoladas. Fazem parte de um processo de definir e manter uma política de segurança da informação efetiva.
- Auditorias envolvem todas as pessoas que utilizam algum recurso computacional através de uma organização.

Trilha de Auditoria

- Existe a necessidade de segurança em sistemas de informação em poder saber quais ações foram executadas e quem as executou.

- Torna-se necessário um mecanismo de gravação e recuperação das ações ou eventos que foram realizados no sistema.

Trilha de Auditoria

A geração trilhas de auditoria, a análise e a forma de armazenamento são definidas de acordo com a necessidade da aplicação e são os principais pontos para o planejamento de um sistema de auditoria.

Processo de Auditoria

- **Que ações devem ser registradas?**

  Registrando tudo, haverá problemas de espaço para tanta informação, lentidão do sistema e acúmulo demasiado de informações.

- **Que informações dessas ações devem ser registradas?**

  Registrando pouco, corre-se o risco de não identificar justamente aquela ação que permitiria desvendar o problema.

Processo de Auditoria

- **O que fazer com a privacidade?**

  Alguns sistemas exigem requisitos de privacidade do usuário.

A auditoria poderá violar a privacidade.
Deve-se ignorar a auditoria para preservar a privacidade?

Processo de Auditoria

- **Como será feita a análise da trilha?**
  Normalmente a trilha somente será analisada em caso de problema de segurança.

- **Como será armazenada a trilha?**

  Um arquivo em disco pode ser uma boa opção, mas uma trilha de auditoria que pode ser apagada pelo atacante detectará apenas os ataques mais simples.

Processo de Auditoria

- **O que fazer quando não houver espaço para registro na trilha?**

  Em todos os modos de armazenamento de trilhas de auditoria existe um limite.

  O que fazer? Apagando-se os registros o sistema estará liberado ao ataque.

Processo de Auditoria

- Excluindo-se os registros mais antigos, o hacker pode descobrir uma ação lícita que gere muitos registros de auditoria e usá-la seguidamente para apagar sua última ação.
- Outra alternativa é bloquear o sistema, impedindo qualquer ação até que o administrador libere mais espaço, sendo a opção mais segura.

Processo de Auditoria

- **Segunda linha de proteção:** por que auditar um evento que o sistema de segurança impede que ocorra?

  Para ser capaz de responsabilizar o usuário em caso de falha das funções de segurança. Se o ativo é importante, já devem existir mecanismos ou procedimentos que impedem o usuário de atingir este ativo.

Processo de Auditoria

- **Melhoria do sistema:** deseja-se medir o funcionamento dos mecanismos de proteção e identificar falhas na proteção, de forma a definir possíveis pontos de melhoria do sistema.

- **Aumento de escopo:** precisa-se identificar seqüências de ações que, embora válidas isoladamente, geram prejuízos ou exposição desnecessária de ativos.

Processo de Auditoria

- **Prevenção:** necessidade de aviso de tentativas de invasão ou ameaças que tentem repetidamente fraudar os mecanismos de segurança do sistema.

- **Política:** atendimento à determinação da política de segurança.

Obrigado!