


Outros Conceitos

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br

Gestão de Segurança




Roteiro

- Ameaças
- Ataques
- Vulnerabilidades

Marcos Laureano

2

Gestão de Segurança



Ameaças

- do inglês *threat*
- qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa
- explora uma vulnerabilidade
 - só existem ameaças se existirem vulnerabilidades

Marcos Laureano

3

Gestão de Segurança

Ameaças

- Inteligente
 - adversário com potencial técnico e operacional
- Ameaça
 - circunstância que poderia romper a segurança
- Análise
 - estudo das probabilidades
- Conseqüências
 - violação da segurança

Marcos Laureano

4

Gestão de Segurança

Classificação de ameaças

- Naturais
 - fenômenos da natureza
- Involuntárias
 - inconscientes, ignorância do usuário, falta de energia, acidentes
- Voluntárias
 - propositais causadas por agentes humanos

Marcos Laureano

5

Gestão de Segurança

Ameaças

- Outras ameaças
 - Falha de hardware ou software
 - Roubo de dados, serviços, equipamentos
 - Incêndio
 - Mudanças no programa
 - Problemas de telecomunicação
- Podem se originar de fatores técnicos, organizacionais e ambientais
 - agravados por más decisões administrativas

Marcos Laureano

6

Gestão de Segurança

Ataques

- Do inglês *attack*
- assalto ao sistema de segurança
 - derivado de uma ameaça inteligente
- ato de tentar desviar os controles de segurança
 - quebrando os princípios de segurança
- o fato de estar acontecendo não significa sucesso
 - depende dos níveis de vulnerabilidades

7

Gestão de Segurança

Ataques

- Ativos
 - alteração dos dados
- Passivos
 - liberação / observação dos dados
- Destrutivos
 - negando acesso aos dados

8

Gestão de Segurança

Classificação de Ataques

- Interceptação
 - acesso por entidades não autorizadas
- Interrupção
 - do fluxo normal
- Modificação
- Personificação
 - acesso/transmissão se passando por uma entidade autêntica

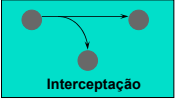
The diagrams show: 1. Interceptação: A yellow box (attacker) is positioned between two blue boxes (sender and receiver), with an arrow pointing from the sender to the attacker. 2. Modificação: A yellow box (attacker) is positioned between two blue boxes (sender and receiver), with an arrow pointing from the sender to the attacker and another arrow pointing from the attacker to the receiver. 3. Interrupção: A yellow box (attacker) is positioned between two blue boxes (sender and receiver), with an arrow pointing from the sender to the attacker and another arrow pointing from the attacker to the receiver, but the main flow is blocked. 4. Personificação: A yellow box (attacker) is positioned below two blue boxes (sender and receiver), with an arrow pointing from the attacker to the receiver, and another arrow pointing from the sender to the receiver.

9

Gestão de Segurança

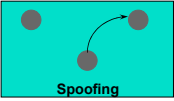
Ataques x Propriedades

Privacidade



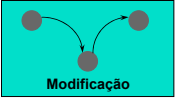
Intercepção

Autenticidade



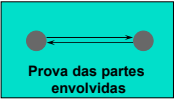
Spoofing

Integridade



Modificação

Não Repúdio



Prova das partes envolvidas

10

Gestão de Segurança

Vulnerabilidades

- Ponto onde qualquer sistema é suscetível a um ataque
 - condição encontrada em determinados recursos, processos, configurações, etc.
- Todos os ambientes são vulneráveis
 - princípio de que não existem ambientes totalmente seguros.

11

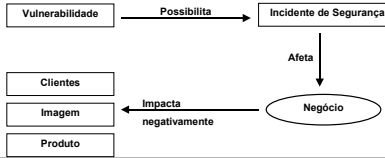
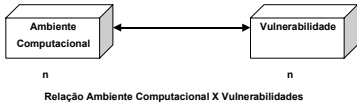
Gestão de Segurança

Vulnerabilidades

- estão presentes no dia-a-dia das empresas
 - se apresentam nas mais diversas áreas de uma organização
 - encontramos nas medidas implementadas pela empresa
- Não existe uma única causa para surgimento de vulnerabilidades
 - negligência
 - ignorância

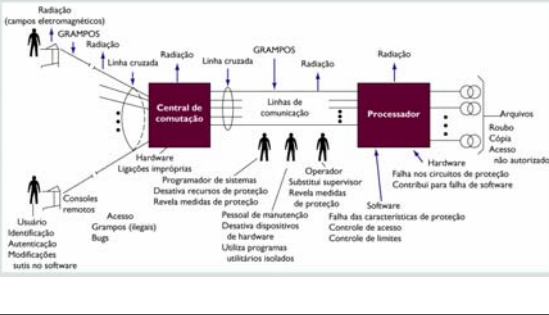
12

Vulnerabilidades



Marcos Laureano

Por que sistemas são vulneráveis ?



Marcos Laureano

Então....

- Dúvidas ??
- Perguntas ??
- Comentários ??

Marcos Laureano
