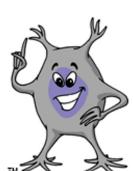
#### Unicap

# Segurança e Auditoria em Sistemas



# O que veremos hoje....

- Introdução à:
  - Segurança em Redes
  - Segurança de Sistemas

# Recursos da Informação

Um arquivo.

Objetos.

Um banco de dados.

## Valor da Informação

Muitos recursos de informação que são disponíveis e mantidos em sistemas distribuídos através de redes, têm um alto valor intrínseco para seus usuários.

Toda informação tem valor e precisa ser protegida contra acidentes ou ataques.

## Segurança

# É uma disciplina complexa e pode abranger várias situações, tais como:

- Erros,
- Acesso indevido,
- Furto,
- Fraude,
- Sabotagem e
- Causas da Natureza.

### Segurança

Com o advento das redes de computadores e a intensificação do uso dessas pelas empresas, a segurança da informação tem sido um assunto que vem exigindo, cada vez mais, maiores cuidados do que aqueles até então existentes antes das redes.

#### Mercado

corporativo: tecnologias avançadas com alta capacidade de tráfego e gerenciamento dos recursos de informação.

Segurança voltada para o mercado doméstico: usuário da Internet.

## Mercado Corporativo

#### A segurança pode ser estudada visando-se:

#### Segurança em Redes:

- Criptografia,
- Autenticação,
- Protocolos,
- Plataformas.

#### Segurança de Sistemas

- Firewall,
- Vírus,
- Cavalos de Tróia
- entre outros...

## Porque ...?

Os sistemas computacionais ou de comunicação, que armazenam ou transmitem informação são vulneráveis (sujeito a intrusões).

#### O Conceito de Intrusão

Análise da Vulnerabilidade (descobrir o melhor caminho para chegar até a invasão).

Preparação das Ferramentas (constrói ou escolhe as ferramentas para a invasão).

Ameaça ou Tentativa (quando o invasor pula o muro).

Ataque (concretiza o arrombamento).

Invasão ou Penetração (quando obtém sucesso).

## Vulnerabilidade - "Pontos Fracos"

Uma falha de segurança em um sistema de software ou de hardware que pode ser explorada para permitir a efetivação de uma intrusão.

# Ameaça (Threat) - "Pulando o Muro"

É a tentativa de ataque a um sistema de informação, explorando suas vulnerabilidades, no sentido de causar dano à confidencialidade, integridade ou disponibilidade.

Pode ser intencional ou não-intencional.

# Ataque (Attack) - "Arrombamento"

O ato de tentar desviar dos controles de segurança de um sistema de informação.

Qualquer ação que comprometa a segurança da informação de propriedade de uma organização.

### **Ataques**

Pode ser ativo, tendo por resultado a alteração dos dados.

Pode ser passivo, tendo por resultado a obtenção da informação (escuta oculta de transmissões): liberação de conteúdos de mensagens, análise de tráfico)

### **Ataques**

Pode ser externo, quando originado de fora da rede protegida.

Pode ser interno, quando originado de dentro da rede protegida.

#### **Ataques**

O fato de um ataque estar acontecendo, não significa necessariamente que ele terá sucesso.

O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficiência das contramedidas de segurança existentes (se não forem suficientemente eficientes).

#### Contramedidas

Mecanismos ou procedimentos colocados num sistema para reduzir risco.

Risco proveniente de vulnerabilidades ameaças, e impacto.

### **Impacto**

A consequência para uma organização da perda de:

- confidencialidade
- disponibilidade
- integridade de uma informação.

### **Impacto**

- O impacto deve ser analisado quanto à
  - modificação,
  - destruição,
  - divulgação ou
  - negação de informação.

Relaciona-se a imagem da empresa, ao dano, a perdas financeiras ou legais e a outros problemas que podem ocorrer como consequência de uma ruptura da segurança.

## Invasão / Penetração...?

Obtenção da Informação.

Acesso bem sucedido, porém não autorizado, em um sistema de informação.

## Os Requisitos de Segurança

- Disponibilidade
- Privacidade (\*\*)
- Confidencialidade
- Integridade
- Autenticidade
- Controle de Acesso
- Não-Repúdio da Informação

#### Unicap

# Dúvidas?

