Parte II

VISÃO GERAL DOS RISCOS

VULNERABILIDADES

- Ausência de proteção cobrindo uma ou mais ameaças.
- Fraquezas no sistema de proteção.
- Não importa a definição usada, vulnerabilidades são claramente associadas com ameaças.

Exemplos

- A **ameaça a acesso não autorizado** está ligada a **controles de acesso inadequados**.

- A **ameaça de perda de dados críticos** e apoio ao processamento se deve ao **planejamento de contingência ineficaz**.

Exemplo

- A ameaça de incêndio está associada a vulnerabilidade da prevenção contra incêndio inadequada.

Bens

- **Bens Tangíveis**

  Aqueles que são paupáveis: HW, SW, suprimentos, documentações, ...

- **Bens Intangíveis**

  Pessoa, reputação, motivação, moral, boa vontade, oportunidade, ...

Bens

- Os bens mais importantes são as **informações**.
- **Informações** ficam em algum lugar entre os bens tangíveis e os intangíveis.

Informações Sensíveis

- Informações, que se perdidas, mal usadas, acessadas por pessoas não autorizadas, ou modificadas, podem prejudicar uma organização, quanto funcionamento de um negócio, ou a privacidade de pessoas.

Ameaças

- Uma ameaça é um evento que acarreta algum perigo a um bem.

- Evento é um fato causador de perda.

Agente da Ameaça

- É uma entidade que pode iniciar a ocorrência de uma ameaça.

- Entidade: uma pessoa:

  o invasor, o intruso

Ameaças Não Intencionais

- Erros humanos,
- Falhas em equipamentos,
- Desastres naturais,
- Problemas em comunicações.

Ameaças Intencionais

- Roubo,
- Vandalismo,
- Utilização de recursos, violando as medidas de segurança

Consequências

- Referem-se aos resultados indesejados da ação (ocorrência) de uma ameaça contra um bem, que resulta em perda mensurável para uma organização.

- Quase todo risco tem consequência, embora de difícil previsão.

Risco

- É uma medida da probabilidade da ocorrência de uma ameaça.
- É a probabilidade do evento causador de perda ocorrer.
- Oficialmente, um risco corresponde ao grau de perda.

Ameaças, Riscos

- Ameaças variam em severidade.
- **Severidade**: grau de dano que a ocorrência de uma ameaça pode causar a um sistema.
- Riscos variam em probabilidade.

Objetivo da Segurança da Informação

- Controlar o acesso às informações.
- Somente pessoas devidamente autorizadas devem estar habilitadas a apreciar, criar, apagar ou modificar informações.

Controle de Acesso impõe quatro requisitos

- (1) Manter confidenciais informações pessoais sensíveis.
- (2) Manter integridade e precisão das informações e dos programas que a gerenciam.

Controle de Acesso impõe quatro requisitos

- (3) Garantir que os sistemas, informações e serviços estejam disponíveis (acessíveis) para aqueles que devem ter acesso.

- (4) Garantir que todos os aspectos da operação de um SI estejam de acordo com as leis, regulamentos, licenças, contratos e princípios éticos estabelecidos.

Sobre requisitos

- Impedir acesso a alguns usuários (requisito 1) e autorizar fácil acesso a outros (requisito 3) requer **filtragem** muito bem feita.

- **Filtragem**, corresponde a introdução de **controles de segurança** que visem a reduzir riscos.

Controles e Proteções

- **Controles** são esforços que reduzem a probabilidade associada aos riscos.

- **Proteções** são controles físicos, mecanismos, políticas, ou seja, procedimentos que protegem os bens de ameaças.

- **Exemplos de proteção**: alarmes, senhas, controles de acesso.

Proteções

- Os tipos de proteções selecionados dependem da função pretendida dos bens e valores.
- Na indústria privada ou repartições do governo, a **disponibilidade** e a **integridade** dos bens podem ser a preocupação básica.
- No meio militar, a **confidencialidade** pode ser mais importante.

Custos das Medidas

- Os gastos com segurança devem ser justificados como qualquer outro.

- A chave para selecionar medidas de seguranças adequadas é a habilidade de estimar a redução em perdas depois da implementação de certas proteções.

Custo-Benefício

- Uma análise de custo-benefício permite justificar cada proteção proposta.

- O custo das medidas de segurança deve ser sempre inferior ao valor das perdas evitadas.

Exposições

- **Exposições** são áreas com probabilidade de “quebra” maior que outras.

Objetivos do Especialista em Segurança

- Apresentar **controles para modificar as exposições**, de modo que todos os eventos de determinada severidade tenham a mesma probabilidade.

- **Minimizar o custo de controles**, ao mesmo tempo, **maximizando a redução de exposições**.

Gerenciamento de Riscos

- Engloba o espectro de atividades, incluindo os controles, procedimentos físicos, técnicos e administrativos, que levam a soluções de segurança de baixo custo.

Gerenciamento de Riscos

- Procura obter as proteções mais efetivas contra ameaças intencionais (deliberadas) ou não intencionais (acidentais) contra um sistema computacional.

Gerenciamento de Riscos

- Tem quatro partes fundamentais.

- **Análise de Risco** (determinação de risco)
- **Seleção de Proteção**
- **Certificação e Credenciamento**
- **Planejamento de Contingência**

Análise de Risco

- Pedra fundamental da gerência de riscos.
- Procedimentos para estimar a probabilidade de ameaças e perdas que podem ocorrer devido a vulnerabilidade do sistema.
- O propósito é ajudar a detectar proteções de baixo custo e prover o nível de proteção necessário.

Seleção de Proteção

- Os gerentes devem selecionar proteções que diminuem certas ameaças.

- Devem determinar um nível de risco tolerável e implementar proteções de baixo custo para reduzir perdas em nível aceitável.

Seleção de Proteção

- As proteções podem atuar de diversos modos:
  - Reduzir a possibilidade de ocorrência de ameaças.
  - Reduzir o impacto das ocorrências das ameaças.
  - Facilitar a recuperação das ocorrências das ameaças.

Seleção de Proteção

- A gerência deve focalizar áreas que têm grande potencial para perdas.

- As proteções devem ter boa relação custo-benefício, isto é, trazer mais retorno que os gastos com implementação e manutenção.

Certificação e Credenciamento

- Podem ser importantes elementos da gerência de risco.
- Certificação é verificação técnica de que as proteções e controles selecionados são adequados e funcionam corretamente.

Certificação e Credenciamento

- **Credenciamento** é a autorização oficial para operação, correções de segurança ou suspensão de certas atividades.

Planejamento de Contingência

- Eventos indesejados acontecem, independente da eficiência do programa de segurança.

Planejamento de Contingência

- É um documento ou conjunto de documentos que permitem ações antes, durante, e depois da ocorrência de evento não desejado (desastre) que interrompe operações da rede.

- Permite uma resposta controlada que minimiza danos e recupera operações o mais rápido possível.

Ameaças à Segurança de Rede

- Exemplos (material escrito, distribuído em aula)
- Caracterizando ameaças.
- Examinar as ameaças possíveis à uma rede (material escrito).