VISÃO GERAL DOS RISCOS

Pensando em Ameaças e 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**.

Um outro exemplo

- A ameaça de incêndio está associada a vulnerabilidade da prevenção contra incêndio inadequada.
- Ameaças podem atingir determinados bens.

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.
- Exemplo de evento-ameaça: um email de autenticidade forjada com um cavalo de tróia.

Agente de uma Ameaça

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

- Entidade: uma pessoa (o invasor, intruso).

  (desastres naturais, incêndio, falha de HW ???)

- Em todas as ameaças deste capítulo, uma pessoa é o agente do erro e um computador a vítima.

Ameaças Não Intencionais

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

Ameaças Intencionais

- Furto de informação,
- 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.

Risco

- É uma **medida da probabilidade** da ocorrência de uma ameaça.
- É a probabilidade do evento causador de perda ocorrer.
- Um risco corresponde ao grau de dano.
- Quase todo risco tem uma consequência, que pode ser de difícil previsão.

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 (acessibilidade) 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 (ética).

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.

Exemplos de Ameaças aos Quatro Requisitos

Confidencialidade
Integridade
Acessibilidade
Leis / Ética

- Cavalos de Tróia
- Vírus
- Worms
- Vazamento de Informações
- Elevação de Privilégios
- Pirataria
- Emanações
- Falhas de Hardware
- Fraude

- Falsificação
- Backdoor
- Erros Humanos
- Impedimento de Uso
- Desfalque
- Informações Imprecisas
- Incêndios ou Desastres Naturais
- Bombas Lógicas
- Erro de Representação

- Danos intencionais em dados ou programas.
- Sniffers
- Sobrecarga
- Entrada Inesperada
- Erros de Programação
- Sabotagem
- Controle de versão.
- Furto

Cavalo de Tróia

- Programa que se apresenta executando uma tarefa e na realidade faz outra.

- Ameaça à: C, I, A.
- Prevenção: muito difícil.
- Detecção: pode ser muito difícil.
- Severidade: potencialmente muito elevada.

Vírus

- É um programa que infecta outros programas por modificá-los. A modificação inclui uma cópia do vírus, o qual pode então infectar outros.
- Ameaça à: I, A
- Prevenção: pode ser difícil.
- Detecção: normalmente imediata.
- Severidade: pode ser baixa ou potencialmente muito elevada.

Worms

- É um programa de rede que usa conexões de rede para se espalhar de sistema a sistema.
- Uma vez ativo, dentro de um sistema, um *worm* pode comportar-se como a vírus, pode implantar programas cavalos de tróia ou realizar qualquer ação destrutiva.
- Um *worm* se replica usando algum veículo de rede: facilidade de email, capacidade de execução remota e capacidade de *login* remoto.

Worms

- Ameaça à: Integridade, Acessibilidade.
- Prevenção: pode ser difícil.
- Detecção: normalmente imediata, através de antivírus.
- Severidade: pode ser baixa ou potencialmente muito elevada.

Pirataria de Software

- Cópia ilegal de software e documentação e reembalagem para comercialização.
- Ameaça à: Leis / Ética
- Prevenção: muito difícil.
- Detecção: Pode ser difícil.
- Frequência: extremamente comum.
- Severidade: Potencialmente muito elevada.

Erros de Programadores

- Erros naturais de programação ao codificar, provocando *bugs* em proporções alarmantes.
- Ameaças à: C, I, A
- Prevenção impossível.
- Detecção: às vezes difícil
- Frequência: comum.
- Severidade: potencialmente muito elevada.

Sniffers

- Programas que podem ler qualquer aspecto de tráfego em uma rede, como por exemplo, capturando senhas, emails e arquivos.
- Ameaça à: Confidencialidade.
- Prevenção: impossível.
- Detecção: possivelmente detectados.
- Severidade: potencialmente muito elevada.

Desfalque

- Normalmente se refere a furto de dinheiro.
- Ameaça à: integridade e recursos.
- Prevenção: difícil.
- Detecção: pode ser difícil.
- Frequência: desconhecida.
- Severidade: potencialmente muito elevada.

Fraude

- Qualquer exploração de sistema de informação tentando enganar uma organização ou tomar seus recursos.
- Ameaça à: Integridade.
- Prevenção: difícil.
- Detecção: difícil.
- Frequência: desconhecida.
- Severidade: potencialmente muito elevada.

Falsificação

- Criação ilegal de documentos ou registros, intencionalmente produzidos como reais.
- Ameaça à: I e outros recursos.
- Prevenção: pode ser difícil.
- Detecção: pode ser difícil.
- Frequência: desconhecida.
- Severidade: potencialmente muito elevada.

Backdoor

- Um programa que é colocado numa máquina, como se fosse um serviço associado a uma porta, mas que tem a incumbência de fazer uma intrusão.
- Ameaça à: C. I, A.
- Prevenção: muito difícil.
- Detecção: possivelmente detectável.
- Severidade: potencialmente muito elevada.

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, biometria, métodos de autenticação.

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 (ou danos que podem ser causados).

Exposições

- **Exposições** são “áreas” (redes, máquinas, ...) 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**
- **Verificação Técnica**
- **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.

Verificação das Proteções

- Verificação técnica de que as proteções e controles selecionados são adequados e funcionam corretamente.

- Importante em gerência de risco.

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.

Causas quase catastróficas ou catastróficas

- Utilização de Dados de Teste em ambientes produtivos.
- Software prejudicial intencional.
- Incêndio, inundação.
- Falha de Periférico.
- Falha de Comunicação.
- Furto de bens físicos.
- Defeito na fonte energia, picos de tensão.

Plano de Contingência

- Deve detalhar:

  - responsabilidades
  - ações antes da ocorrência ...
  - ações durante ...
  - ações de recuperação ...
  - ações para restabelecer operações normais de uma rede.