Capítulo 2

Pensando em Vulnerabilidades, Ameaças e Riscos

Objetivos

- Avaliar ameaças e riscos à segurança de redes.
- Após concluir este capítulo, você estará preparado para executar as seguintes tarefas:

Tarefas

- Identificar as necessidades de segurança de rede.
- Identificar algumas das causas dos problemas de segurança de rede.
- Identificar características e fatores motivadores de invasão de rede.

Tarefas

- Identificar as ameaças mais significativas na segurança de rede.
- Conceituar vulnerabilidade, ameaça, risco e gerenciamento de risco.

Por que segurança ... ?

- Porque para garantir a segurança nos negócios é preciso atualizar constantemente as defesas para reduzir a vulnerabilidade às ameaças inovadoras dos invasores.

Desafios

- **Segurança** é difícil de ser implementada uniformemente em toda a empresa.
- Escolha de uma alternativa ou combinação adequada de diversas opções de soluções.

Desafios

- Escolher entre várias opções diferentes e disponíveis e adotar aquelas que satisfaçam os requisitos exclusivos da rede e dos negócios.

Desafios

- Os produtos diferentes devem ser integrados em toda a empresa a fim de se atingir uma única política de segurança estável.

Porque temos problemas de segurança

- Fragilidade da Tecnologia
- Fragilidade de Configuração
- Fragilidade da Política de Segurança

Fragilidade da Tecnologia

- TCP/IP
- Sistema Operacional
- Equipamentos de Rede

Fragilidade de Configuração

- São problemas causados pelo fato de **não se configurar equipamentos interligados** para impedir problemas de segurança conhecidos ou prováveis.

Fragilidade de Configuração

- Considerações *default* inseguras nos produtos.
- Equipamento de rede configurado equivocadamente.
- Contas de usuários inseguras.
- Contas de sistemas com senhas previsíveis.

Fragilidade do Equipamento de Rede

- Proteção de senha insegura
- Falhas de autenticação
- Protocolos de Roteamento
- Brechas no Firewall

Fragilidades da Política de Segurança

- Falta de uma política escrita.
- Políticas internas
- Falta de continuidade dos negócios
- Controles de acesso para equipamentos de rede não são aplicados.
- A administração de segurança é negligente, inclusive a monitoração e a auditoria.

Fragilidades da Política de Segurança

- Falta de conhecimento sobre ataques.
- Alterações e instalação de software e hardware não seguem a política.
- Falta de Planejamento de Contingência.

Conheça seus invasores

- **Script Kiddie**

  Não possuem muita habilidade.

  Mas teve a sorte de encontrar um sistema remoto que não aplicou o *patch* de correção a tempo.

Script Kiddie

- São bons na razão inversamente proporcional à negligência de administradores/usuários que não acompanham listas de segurança e demais páginas de fornecedores ou CERT (Computer Emergency Response Team)

Script Kiddie

- Um invasor que faz intrusão vinculada a uma falha conhecida.
- Não buscam informações e/ou máquinas específicas. Ou seja, ganhar acesso de root.
- Basta ter acesso para desconfigurar home pages de forma mais fácil possível.

Script Kiddie

- Sua técnica consiste em ficar revirando a Internet atrás de máquinas vulneráveis e fazer explorações com *exploits,* ferramentas que permitam explorar as falhas em serviços.

Script Kiddie

- Podem desenvolver suas próprias ferramentas.
- Existem os que não conhecem nenhuma técnica, e tudo o que sabem é executar as ferramentas fornecidas por outro script kiddie.

Cracker

- Um invasor de bons conhecimentos técnicos e assim sendo, ele será capaz de apagar seus rastros de maneira mais sutil.

- Se caracteriza pelo alto nível técnico, na medida em que cada passo da invasão é realmente estudado e bem pensado.

Cracker

- Busca dados como configurações padrões ou senhas padrões que ele possa explorar.
- Tem capacidade para desenvolve seus próprios *exploits*. São geniais e criativos para a má intenção.
- Realiza ataques inteligentes para comprometer a segurança da rede.

Cracker

- Suas atitudes furtivas poderão enganar até aos mais experientes administradores.
- São os verdadeiros invasores (intrusos) ou até mesmo criminosos cibernéticos.

Hacker

- Um programador apaixonado.
  Constroem e tornam o mundo melhor.

  Exemplos:

  Stallman, Linus Torvalds, Ada Lovelace, Douglas Engelbart, Dennis Ritchie, Ken Thompson, Arnaldo Melo, Marcelo Tossati, Alan Cox, ...

  Não são fúteis desconfiguradores de páginas.

Hacker

- (Hacking ou Hacking Ético)

  Programador ou administrador que se reserva a questionar os problemas de segurança nas tecnologias disponíveis e as formas de provar o conceito do que é discutido.

Hacker Ético

- Uma pessoa que investiga a integridade e a segurança de uma rede ou sistema operacional.
- Usa o conhecimento avançado sobre SW e HW para entrar no sistema através de formas inovadoras.

Hacker Ético

- Compartilha seu conhecimento gratuitamente através da Internet.
- Não usa de más intenções. Tenta oferecer um serviço à comunidade interessada.

Conceito de Invasor

- Script Kiddie
- Cracker
- Hacker
- Phracker (pessoas que fazem acesso não autorizado a **recursos de telecomunicações**)

Características de um Invasor

- Sabem codificar em várias linguagens de programação.
- Conhecimentos aprofundados sobre ferramentas, serviços e protocolos.
- Grande experiência com Internet.
- Conhecem intimamente pelo menos dois Sos.

Características de um Invasor

- Têm um tipo de trabalho que usa redes. Usam equipamentos como se fossem modo de vida.
- Colecionam SW e HW.
- Têm vários computadores para trabalhar.

Motivos para ameaças

- Exploração de emoções (Notoriedade, Diversão).
- Concorrência de mercado
- Inimigos políticos
- Ladrões (atividades furtivas)
- Espiões (Espionagem industrial)

Motivos para ameaças

- Funcionários hostis:

  empregados ou antigos empregados, vingança, ataque de Troca de Senhas ou Sessões Abertas)

- Investigação legal.

Vulnerabilidades

- Ausência de proteção cobrindo uma ou mais ameaças.
- Fraquezas no sistema de proteção.
- **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 ao funcionamento de um negócio ou a privacidade de pessoas.

O que é uma **ameaça** ?

- Uma **ameaça** é algum fato **que pode ocorrer e acarretar algum perigo** a um bem.
- Tal fato, se ocorrer, será causador de perda.
- É a **tentativa de um ataque**.

Agente de uma ameaça

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

- Entidade: uma pessoa:

  invasor / intruso

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.

Impacto

- Resultados indesejados da ocorrência de uma ameaça contra um bem, que resulta em perda mensurável para uma organização.

- Quase todo **risco** tem um impacto, 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, Severidade

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

Tipos de Ameaças à Segurança

- Acesso não-autorizado
- Reconhecimento
- Recusa de Serviço
- Manipulação de Dados

Acesso Não-Autorizado

- Objetivo: obter acesso como administrador num computador remoto.
- Controlar o computador de destino e/ou acessar outros interligados.

Formas de Acesso Não-Autorizado

- Acesso inicial
- Com base em senhas
- Privilegiado
- Acesso secundário
- Permissão de acesso remoto
- Vulnerabilidades de programa
- Arquivos não autorizados

Reconhecimento

- Monitoramento de vulnerabilidades, serviços, sistemas ou tráfego de rede, no sentido de levantar informações visando um ataque futuro.

Formas de Reconhecimento

- Varreduras de porta

- Investigação:
  - observação passiva do tráfego de rede com um utilitário, visando padrões de tráfego ou capturar pacotes para análise e furto de informação.
  - *Snooping* de rede (*sniffing* de pacotes)

Recusa de Serviço

- Denial of Service (DoS)
- Tentativa de desativar ou corromper serviços, sistemas ou redes, no sentido de impedir o funcionamento normal.

Formas de Recusa de Serviço

- Sobrecarga de recurso
- Distributed Denial of Service
- Bombas de email

Manipulação de Dados

- Captura, alteração e repetição de dados através de um canal de comunicação.
- Falsificação de IP
- Repetição de sessão
- Repúdio

Falsificação de IP

- Ocorre quando um invasor da fora de uma rede, finge ser um computador confiável dentro da rede.

- O IP usado está dentro do intervalo da rede invadida, ou é usado um IP externo autorizado, confiável, e para o qual é disponibilizado acesso a recursos na rede.

Falsificação de IP

- Ocorre através da manipulação de pacotes IP.
- Um endereço IP de origem de um computador confiável, é falsificado para assumir identidade de uma máquina válida, para obter privilégios de acesso no computador invadido.

Segurança da Informação

- Somente **pessoas devidamente autorizadas** devem estar habilitadas a **ler**, **criar**, **apagar** ou **modificar** informações.

- **Controlar o acesso** às informações.

Controle de acesso: quatro requisitos

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

Controle de acesso: 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.

Exemplos de Ameaças aos Quatro Requisitos

Confidencialidade
Integridade
Acessibilidade
Leis / Ética

Ameaças

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

Ameaças

- Falsificação
- Backdoor
- Desfalque
- Incêndios ou Desastres Naturais

Ameaças

- Erros de Programadores
- Sniffers
- Entrada Inesperada
- Furto de informação

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 usa conexões de rede para se espalhar de sistema a sistema.
- Uma vez ativo, um *worm* pode comportar-se como a vírus, pode implantar programas cavalos de tróia ou realizar qualquer ação destrutiva.
- Um *worm* se replica usando 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 re-embalagem 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 um 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 procedimentos ou medidas que reduzem a probabilidade associada aos riscos.
- **Proteções** são controles físicos, mecanismos, ou políticas, que protegem os bens de ameaças.
- **Exemplos de proteção**: alarmes, senhas, controles de acesso.

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 da rede com probabilidade de **“quebra”** maior que outras.

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

- 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**
- **Plano de Contingência**

Análise Risco

- Pedra fundamental da gerência de riscos.
- Procedimentos para estimar a probabilidade de ameaças e perdas que podem ocorrer devido a vulnerabilidade do sistema.

Análise de Risco

- 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

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

Credenciamento

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

Plano de Contingência

- Eventos indesejados acontecem, independente da eficiência do programa de segurança.
- Permite uma resposta controlada que minimiza danos e recupera operações o mais rápido possível.

Plano 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.

Avaliando ameaças

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