Curso de Tecnologia em Redes de Computadores
Disciplina: Auditoria e Análise de Segurança da Informação - 4º período
Professor: José Maurício S. Pinheiro

AULA 6: Segurança e Confiabilidade

A questão da segurança e confiabilidade do sistema computacional faz parte do cotidiano do auditor e analista de segurança, fato que o impele a buscar o aprimoramento de seus conhecimentos para que não seja surpreendido com novas táticas e técnicas de invasão irremediavelmente destruidoras.

Ao analisar os aspectos de segurança e confiabilidade de uma rede de computadores uma série de perguntas deve ser feita para se determinar o nível de investimentos que deverá ser feito na segurança do sistema computacional (Figura 1):

- Os sistemas envolvidos estão seguros?
- Os usuários estão conscientes para com os aspectos gerais de segurança?
- A base de dados está segura e mantém a sua inviolabilidade e preserva a confiabilidade dos dados?
- A intranet e extranet são protegidos contra violações e interceptações de mensagens?
- A proteção existente é suficiente ou ainda faltam conhecimentos para operacionalizar níveis de segurança que possibilitem serviços de qualidade, com a abertura requerida, confiabilidade e com segurança?

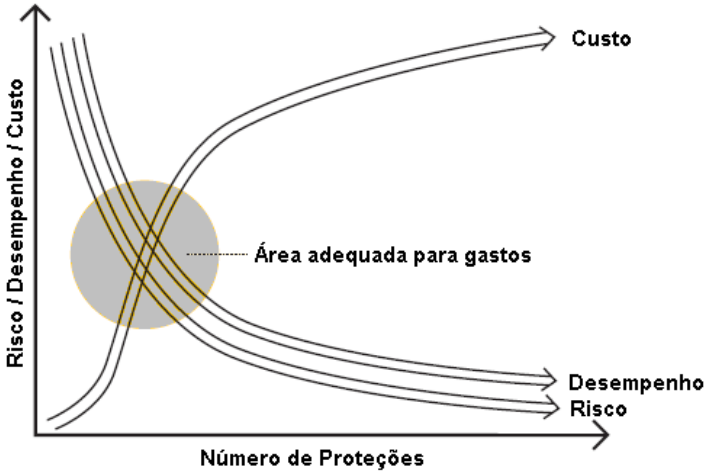

Figura 1 - Determinando os níveis de investimentos em segurança

Em termos simples, define-se segurança como a inexistência de perigo ou risco de perda. O principal problema para implementar uma cultura de segurança está nas pessoas envolvidas no processo, pois é preciso mostrar para elas que os equipamentos devem ser protegidos, que as senhas não devem ser divulgadas e que as informações confidenciais não devem estar disponíveis. Então, a segurança de uma rede de computadores é uma relação de confiança onde os esforços estão direcionados para protegê-la do perigo ou do risco da perda de informações ou dados.

O termo “confiança” é freqüentemente usado com referência a segurança de rede. Pode-se definir um sistema confiável como sendo "aquele que consiste apenas

de componentes independentes, instalados de tal modo que protejam o usuário e a informação e lhes dê um nível apropriado de garantia".

1. Segurança de Rede

Por definição “dado é a unidade básica do conhecimento humano” e “informação é o conhecimento adquirido a partir do processamento de um conjunto de dados. Estas duas definições estabelecem outras duas suposições sobre a segurança de uma rede:

- A rede contém informações e recursos valiosos que são críticos para a organização;
- Os dados e recursos da rede são valiosos e por isso devem ser protegidos.

As redes correm riscos por pelo menos três razões principais:

- Podem ser atacadas por vários pontos;
- Adicionando novos equipamentos a uma rede, aumentamos o perímetro do sistema computacional;
- Computadores em rede oferecem vários serviços que são difíceis de serem protegidos.

A segurança de uma rede de computadores deve ser concebida de modo a manter a confidencialidade, integridade, e disponibilidade das informações que por ela trafega, considerando:

- **Confidencialidade** — o sistema possui confidencialidade quando somente usuários devidamente autorizados podem ter acesso aos seus dados;
- **Integridade** — o sistema possui integridade quando somente usuários autorizados podem modificar os dados;
- **Disponibilidade** — o sistema possui disponibilidade quando os seus dados são acessados pelos usuários autorizados sempre que necessário.

2. Identificação e Autenticação

Para assegurar que apenas pessoas ou computadores autorizados possam acessar ou modificar os dados armazenados em uma rede, se deve ter obrigatoriamente a identificação, como método para estabelecer a identidade do usuário no sistema e a autenticação, como meio para verificar a veracidade da identidade do usuário (Figura 2). Estas duas condições estão intimamente relacionadas e são freqüentemente relacionadas em conjunto, contudo descrevem duas funções separadas e distintas:

- **Identificação** — Processo que ocorre durante o *login* inicial quando uma pessoa provê algum tipo de identificação de segurança, como um nome de usuário único, que identifica o mesmo para o sistema "Este é quem eu sou". É uma afirmação de identidade;

- **Autenticação** — Processo de verificação que exige do usuário uma prova de sua identidade, também única, e que comprove a veracidade da mesma para o sistema, tipicamente uma senha, para afirmar que a identidade está sendo assumida pelo seu legítimo dono. A autenticação assegura para o sistema, "Esta é uma informação privada que prova que eu sou quem digo ser". É a prova da identidade.

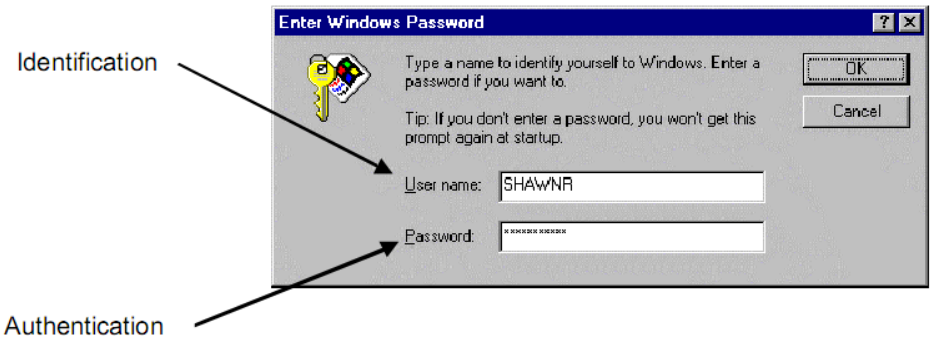

Figura 2 – Exemplo de Identificação e Autenticação

Embora outros métodos de autenticação estejam disponíveis, as senhas ainda são a forma mais comum de autenticação usada nas redes de computadores. Então, um aspecto importante da segurança da rede é a proteção à confidencialidade das senhas para prevenir acessos não autorizados.

3. Autenticação de Usuário e de Host

O nível de autenticação depende da importância do recurso e o custo do método. Uma meta importante a ser atingida através da identificação e da autorização é prover *accountability* (controle de contas de acesso). O controle de contas de acesso é a habilidade do sistema em determinar de modo confiável quem é o usuário, quando ele obtém acesso e registrar suas ações enquanto estiver conectado.

Dois tipos de autenticação com os quais o administrador de redes de computadores deve ter familiaridade são a autenticação de usuário e a autenticação de host:

- **Autenticação de usuário** — Ocorre durante a seqüência de *login* no sistema, normalmente caracterizada como:
    - Algo que o usuário sabe;
    - Algo que o usuário possui;
    - Algo que o usuário é;
- **Autenticação host-to-host** — Ocorre durante a operação do sistema, normalmente caracterizada como:
    - Criptografada;
    - Não criptografada.

3.1. Autenticação de Usuário

A autenticação de usuário (ou cliente) pode ser feita de várias formas através de:

- Senhas;
- *Token*;
- *Smart Cards*;
- Biometria.

3.1.1. Senhas

Como um meio de autenticação pessoal, as senhas se caracterizam como "algo que se sabe". As vantagens de se usar senhas como um meio de autenticação são:

- Baixo custo;
- Facilidade de uso.

As desvantagens são:

- Podem ser descobertas;
- Podem ser capturadas ou roubadas;
- Usuários podem voluntariamente ou involuntariamente revelar suas senhas;
- Os usuários freqüentemente selecionam senhas fáceis de serem descobertas.

Em geral, as senhas isoladamente não são consideradas um mecanismo de autenticação forte, isto é, seguro.

3.1.2. Token

A combinação de "algo que se tem" com "algo que se sabe" permite um nível de segurança mais forte em relação ao uso da senha simples. Pode-se lançar mão de uma técnica conhecida como “senha de uma única sessão”.

Senhas de uma única sessão caracterizam-se como "algo que se possui". A senha de uma única sessão é usada apenas uma vez e após seu uso ela se torna inválida. Esta estratégia provê uma defesa forte contra os ataques de escuta de sessão de identificação. As senhas de uma única sessão podem ser implementadas de vários modos. O mais comum é usando um dispositivo autenticador pessoal (*hand-held*), também chamado de “Ficha” ou *Token*.

A desvantagem é que este dispositivo está sujeito a roubo. A defesa habitual é adicionar uma senha caracterizada como "algo que se sabe", senha que deve ser usada junto com o dispositivo, estratégia usada pelos bancos nos caixas automáticos.

3.1.2.1. Ataques à Senha

Uma rede com baixo nível de segurança oferece a possibilidade de qualquer um utilizar uma estação de trabalho e tentar entrar com um nome de usuário e senha e ter acesso aos recursos do sistema. Os nomes de usuário podem ser obtidos sem muito esforço ou se um nome de usuário atual é conhecido, o atacante só precisa adivinhar a respectiva senha.

Os ataques mais comuns em uma rede de computadores podem ser geralmente de dois tipos: ataque de força bruta e ataque de dicionário. Os ataques de força bruta são, basicamente, ataques que tentam adivinhar a senha. Os ataques de dicionário são um tipo de ataque que emprega uma lista predefinida de combinações comuns em uma tentativa de chegar a um nome de usuário completo e sua senha respectiva.

Figura 3 - Ataque ao sistema

Se o atacante pode ver as ações do usuário no momento do seu *login*, o ataque fica bem mais fácil (Figura 3). Estudos mostram que adivinhar senhas torna-se cada vez mais fácil, simplesmente porque os usuários comumente selecionam senhas facilmente dedutíveis.

3.1.2.2. Políticas de Senhas

A maneira mais eficiente de se prevenir contra ataques de senha é implementar um bom procedimento para criá-las e mantê-las. Os usuários devem ser treinados para proteger as suas senhas criando senhas não-óbvias com um mínimo de caracteres definidos na política de segurança.

Ao estabelecer diretrizes para a criação de senhas nas organizações deve-se atentar para alguns detalhes simples, porém importantes:

- Não permitir um número ilimitado de tentativas de *login*;
- Estabelecer um limite mínimo de caracteres para as senhas;
- Educar os usuários sobre senhas fracas e fortes;
- Estabelecer limites de validade para as senhas.

3.1.3. *Smart Card*

Um *Smart Card* (cartão inteligente) é um dispositivo portátil provido de processamento e memória não volátil que só é acessível pelo *chip* do cartão. Um leitor do cartão pode ser integrado na estação de trabalho do usuário e pode ser capaz de executar *login* e tarefas de autenticação no sistema (Figura 4).

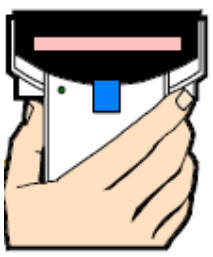

Figura 4 - Leitor de cartão

Os cartões inteligentes podem ser caracterizados como "algo que se tem". Eles normalmente são acrescidos de uma característica do tipo "algo que se sabe", como um número de identificação pessoal (PIN - *Personal Identification Number*).

3.1.4. Biometria

Outro método de autenticação de usuário é conhecido como biometria, que verifica uma característica física única do usuário como uma impressão digital, reconhecimento de voz, assinatura, ou *scan* da retina, por exemplo.

O método biométrico requer hardware especial e que pode apresentar alto custo de aquisição e ser difícil de implementar. A vantagem é que um identificador biométrico não pode ser usado por outra pessoa ou ser roubado.

3.2. Autenticação Host-to-Host

Autenticação Host-to-Host pode ser caracterizada do seguinte modo:

- Autenticação baseada em rede;
- Por técnicas de criptografia.

3.2.1. Autenticação Baseada em Rede

A forma principal de autenticação Host-to-Host na Internet reside na rede. A própria rede carrega a identidade do usuário remoto e presume-se que isto é suficiente para que se tenha uma identidade autenticada.

A Autenticação baseada em rede pode ser feita de dois modos:

- Baseada no endereço — Aceita o endereço IP da fonte;
- Baseada no Nome — Requer um endereço e o nome associado a este endereço.

3.2.2. Técnicas de Criptografia

As técnicas de criptografia proporcionam uma base mais segura para autenticação. As técnicas para realizá-la variam amplamente, mas residem basicamente na posse de informação secreta ou uma chave criptográfica. A posse de informação secreta é equivalente a prova de que se é a pessoa que pode efetuar a autenticação.

As maiores dificuldades encontradas para implementar a autenticação por criptografia são:

- Necessidade de um centro de distribuição de chaves seguro;
- Dificuldade de manter em segredo a chave do host.

4. Controles de Acesso

Em uma rede de computadores são aplicados controles de acesso aos dados que contém as identidades dos usuários do sistema. Estes controles confiam na identificação e autenticação, porque os usuários devem ser identificados e devem ter as suas identidades autenticadas antes do sistema poder estabelecer qualquer

controle de acesso. O controle de acesso protege uma organização de ameaças de segurança especificando e controlando o que pode entrar e sair da rede.

Um elemento chave de controle de acesso é uma visão geral de todos os serviços e aplicações. Neste aspecto, os controles de acesso podem ser caracterizados como:

4.1. Controle de acesso discreto

Restringe o acesso para arquivos ou diretórios baseados na identidade do usuário. Eles são discretos de modo que o dono de um arquivo (ou qualquer usuário com direitos suficientes) é livre para permitir ou revogar o acesso corrente de outros usuários àquele arquivo

4.2. Controle de acesso obrigatório

Restringe acesso por meio de atributos especiais que são fixados pelo administrador da rede e estabelecidos pelo sistema operacional. Estes controles não podem ser evitados ou mudados por usuários não-privilegiados.

O controle de acesso obrigatório está tipicamente baseado em níveis de classificação (*labels*), onde o administrador classifica cada item de informação com um nome como “Não classificado”, “Confidencial”, ou “Secreto”. A cada usuário é designado o acesso a um determinado nível. O sistema operacional então controla o acesso para informação baseado nestas classificações.