Redes de computadores II

Segurança em Redes de Computadores

Conteúdo: Tópicos sobre segurança em redes de computadores

Em se tratando de computadores, “segurança envolve uma série de atitudes que visam proteger a informação contida nos computadores”.

Não podemos tratar de segurança apenas dentro dos computadores, tentamos proteger é a informação que pode residir ou não dentro dos computadores.

De acordo com a norma NBR ISO-IEC 17799:2001, “informação é um ativo que, como qualquer outro ativo importante para os negócios, tem valor para a organização e, consequentemente, necessita ser protegida de maneira adequada”.

Em se tratando de computadores, a informação pode estar nos registros de um banco de dados, num arquivo texto, numa planilha, trafegando por cabos de cobre ou ondas eletromagnéticas, etc. Segurança da Informação abrange todo tipo de informação, computadorizada ou não.

De acordo com a norma NBR ISO-IEC 17799:2001, a segurança da informação consiste na preservação de três características básicas:

- Confidencialidade: a informação só deve ser acessada por pessoas autorizadas
- Integridade: a informação deve estar exata e completa
- Disponibilidade: a informação deve estar acessível sempre que necessária

Segurança da informação abrange outras áreas, entre elas, a **segurança de redes**.

A segurança da informação é tão velha quanto a própria informação, um ano depois da criação do telégrafo, um código de criptografia foi desenvolvido para manter seguras as mensagens transmitidas. Cinco anos após a criação do telefone foi desenvolvido um “embaralhador” de voz para garantir o sigilo das conversas telefônicas. Em 1920, foi criada uma legislação para proibir escutas telefônicas.

Um caso muito famoso na área de estudo de segurança de redes foi quando em 1988, Roberto T. Morris desenvolveu um programa capaz de auto-replicar e se auto-propagar: o Internet Worm.
O programa estava se propagando e infectando máquinas numa velocidade maior que Morris esperava: havia um erro no programa e Morris havia perdido o controle. Ele pediu ajuda a um amigo para encontrar uma solução, mas foi tarde demais: diversos computadores já haviam sido infectados. Esse vírus explorava uma falha no sendmail e no fingerd.
Foram necessárias várias equipes de programadores para conter o worm: enquanto isso várias redes foram desconectadas da Internet, Morris foi condenado a três anos de prisão, 400 horas de serviços comunitários e multa de US$ 10 mil. O worm não acarretava em danos físicos, mas chamou atenção para a fragilidade da Internet.

Princípios básicos de segurança

Com relação à segurança, deve-se utilizar a filosofia de “um dia de cada vez”, “só por hoje”, pois segurança é um processo contínuo, ou seja, um sistema seguro hoje será um sistema vulnerável amanhã.

Um sistema deve ser sempre revisto e atualizado, a cada dia novas vulnerabilidades são descobertas, novas correções são lançadas e novos padrões são definidos.

*Menor privilégio

Esse é um princípio fundamental da segurança e vale para qualquer objeto: usuário, administrador, programa, serviço, etc. Cada objeto deve possuir apenas o mínimo privilégio para realizar suas ações, e nenhum outro. Com isso, limita-se o nível de estrago que um ataque bem sucedido pode causar.

Exemplo:

Visita a uma empresa: acesso somente ao setor informado.

Pergunte-se sempre se não está implementando sistemas com mais privilégios do que devia.

*Defesa em profundidade

A defesa em profundidade consiste em usar mecanismos de defesa em cascata, desse modo, se um mecanismo falhar, haverá um outro em seguida que poderá compensar o que falhou.

Exemplos da vida real:
portas com mais de uma tranca, cartões magnéticos e senhas.

Na computação:
colocar serviços em máquinas separadas.

*Gargalo (Choke Point)

Esse princípio tem o objetivo de obrigar intrusos a utilizar um canal estreito, que pode ser monitorado e controlado, desse modo, todos os acessos devem ser feitos por um único ponto. Pode-se fazer uma analogia na vida real com pedágios, caixas de supermercado, bilheterias, etc.

Na computação, temos como exemplo o firewall, que funciona como um canal estreito que pode ser monitorado e controlado. Qualquer intruso, obrigatoriamente, tem que passar por ele.

O nome “firewall” é uma referência às portas corta-fogo responsáveis por evitar que um incêndio em uma parte do prédio se espalhe facilmente pelo prédio inteiro. Na Informática essa ferramenta previne que os perigos da Internet (ou de qualquer rede não confiável) se espalhem para dentro de sua rede interna.

Um firewall deve sempre ser instalado em um ponto de entrada/saída de sua rede interna, este ponto de entrada/saída deve ser único. O firewall é capaz de controlar todos os acessos de e para a sua rede.

Os objetivos específicos de um firewall são:

- Restringir a entrada a um ponto cuidadosamente controlado.
- Prevenir que atacantes cheguem perto de suas defesas mais internas.
- Restringir a saída a um ponto cuidadosamente controlado.

O firewall pode estar em computadores, roteadores, configuração de redes, software específico, entre outros.

O problema do princípio do gargalo é que basta uma única saída alternativa na sua rede para comprometer todo o seu esquema de segurança.

*Ponto mais fraco

A segurança é como uma corrente: é tão forte quanto o seu ponto (elo) mais fraco, um invasor sabe que provavelmente terá mais sucesso se atacar o ponto mais fraco da sua rede. O administrador deve estar ciente do ponto mais fraco da sua rede, de modo que possa tomar medidas para eliminá-lo ou monitorá-lo. Sempre haverá um ponto mais fraco: muita atenção a ele sem se esquecer dos outros pontos.

*Fail – Safe (Falha segura)

Esse princípio consiste em derrubar um sistema ao menor sinal de invasão. Quando um sistema de segurança falha, deve falhar de tal forma que bloqueie o acesso de um invasor, em vez de deixá-lo entrar. Isso também impedirá o acesso de usuários legítimos.

O sistema pode ficar indisponível até que o reparo seja feito (aceitável, é melhor que uma invasão na rede).

Exemplo:
disjuntor elétrico, travas de elevador para impedir queda.

*Diversidade de defesa

Consiste no uso de sistemas diferentes, o que torna o sistema como um todo mais seguro, pois a vulnerabilidade de um sistema provavelmente não estará presente nos outros. A desvantagem é que isso envolve conhecer sistemas diferentes: complexidade de configuração e de manutenção. Por isso, é necessário analisar a relação custo benefício e sempre lembrar que falhas podem existir em todos os sistemas, mesmo sendo diferentes.

*Simplicidade

Manter as coisas simples faz com que sejam mais fáceis de entender e o entendimento é fundamental para se conhecer o nível de segurança. Programas complexos podem esconder falhas de segurança que são difíceis de encontrar nesse tipos de sistema.

Autenticação e autorização

A **autenticação** consiste no processo de estabelecer a identidade de um indivíduo. Isso requer a identificação e prova desta identificação.
A prova consiste em três categorias: Algo que você sabe, algo que você tem e algo que você é.

Algo que você sabe → Mais simples de implementar, mas oferece menor nível de segurança. Exemplo: senha.

Algo que você tem → Oferece um nível a mais de segurança, o usuário deve possuir algo para se autenticar
Ex: cartão magnético, token USB.
Nesse caso, um invasor pode se fazer passar por um usuário legítimo caso esteja de posse do item necessário.
Outro problema é que esse tipo de autenticação requer hardware especial.

Algo que você é → Mais segura, pois trata-se de características específicas do indivíduo, exemplo: impressão digital, leitura de íris, reconhecimento de voz, uso de dispositivos biométricos, etc.
O problema principal desse tipo de autenticação é o seu custo elevado.

Para deixar o sistema de autenticação mais seguro, pode-se combinar métodos de autenticação distintos.

A **autorização** estabelece o que o usuário pode fazer após a autenticação: Permissões. Aplica-se a qualquer acesso a qualquer recurso (arquivo, dispositivo, rede, chamada de sistema de programação).
Pode-se utilizar criação de perfil, onde o perfil contém todas as permissões para cada recurso que um usuário poderá utilizar.

Detectores de intrusos

IDS – (Intrusion Detection Systems): responsáveis por analisar o comportamento de uma rede ou sistema em busca de tentativas de invasão.

HIDS – (Host IDS): monitora um host específico

NIDS – (Network IDS): monitora uma segmento de rede
Um IDS utiliza dois métodos distintos: detecção por assinaturas detecção por comportamento.

*Detecção por assinaturas

Associam um ataque a um determinado conjunto de pacotes ou chamadas de sistema, não só detecta o ataque como também o identifica. Esse tipo de detecção exige atualizações frequentes do fabricante, semelhante às assinaturas de antivirus.

*Detecção por comportamento

Observa o comportamento da rede em um período normal e o compara com o comportamento atual da rede, quando existe uma diferença significativa entre os comportamentos, o IDS assume que um ataque está em andamento.
Utiliza métodos estatísticos ou inteligência artificial e detecta ataques desconhecidos. O problema desse método é que ele não sabe informar qual ataque está em andamento.

Referências bibliográficas:

TANENBAUM, Andrew. S. Redes de Computadores. São Paulo: *Pearson*, 5ª Ed. 2011.

KUROSE, James F.; ROSS, Keith W. Redes de Computadores e a Internet – Uma Abordagem Top-Down. *São Paulo: Pearson*, 6ª Ed. 2013.

NBR ISO-IEC 17799:2001