# Aspectos de Segurança da Informação

Profº Ed W. Jr

# Aspectos de Segurança da Informação

Profº Ed W. Jr

# Introdução

**Os usuários das redes de computadores mudaram, bem como o uso que os mesmos fazem da rede.**

**A segurança da rede despontou-se como um problema em potencial.**

**O crescimento comercial assustador da Internet nos últimos anos foi superado apenas pela preocupação com a segurança deste novo tipo de mídia.**

**A segurança em sua forma mais simples se preocupa em garantir que pessoas mal intencionadas (externas à empresa, ou internas) não leiam, ou pior, ainda modifiquem dados/mensagens.**

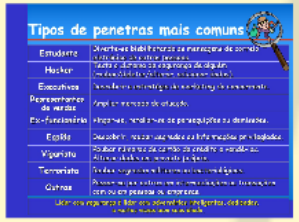
# Política de segurança da empresa

Segundo pesquisas, e constatações feitas pelas próprias empresas especializadas em vender projetos e produtos voltados para o segmento de segurança de informação:

“As empresas brasileiras são vulneráveis, frágeis e passíveis de invasões porque a grande maioria dos executivos – não apenas os responsáveis pela área de tecnologia – adotam posturas paternalistas e não profissionais com relação às informações dentro das corporações”.

Políticas de segurança são responsabilidades dos CIOs, cabendo aos mesmos escreverem as diretrizes, sejam elas agradáveis ou não para os funcionários.

Especialistas reconhecem que cem por cento de segurança é impossível de ser alcançado, todavia é possível alcançar um alto grau de garantia da informação se houver mecanismos de controle diário, 24 horas por dia, sete dias por semana.



# Tipos de penetras mais comuns

| | |
|---|---|
| Estudante | Diverte-se bisbilhotando as mensagens de correio eletrônico de outras pessoas. |
| Hacker | Testa o sistema de segurança de alguém (roubar/deletar/alterar, adicionar dados). |
| Executivos | Descobrir a estratégia de marketing do concorrente. |
| Representantes de vendas | Ampliar mercado de atuação. |
| Ex-funcionário | Vingar-se, retaliar-se de perseguições ou demissões. |
| Espião | Descobrir, roubar segredos ou informações privilegiadas. |
| Vigarista | Roubar números de cartão de crédito e vendê-los. Alterar dados em proveito próprio. |
| Terrorista | Roubar segredos militares ou bacteriológicos. |
| Outros | Passar-se por outros em intermediações ou transações com ou em pessoas ou empresas. |

Lidar com segurança é lidar com adversários inteligentes, dedicados, e muitas vezes bem subsidiado.

# Tipos de ataques

**Implementar uma política de segurança em uma empresa ou organização implica em implementar controles de segurança do tipo:**

- **Físicos;**
- **Lógicos;**
- **Organizacionais;**
- **Pessoais;**
- **Operacionais;**
- **De desenvolvimento de aplicações;**
- **Das estações de trabalho;**
- **Dos servidores;**
- **De proteção na transmissão de dados.**

O desenvolvimento de uma política de segurança deve ser uma atividade interdepartamental.

As áreas afetadas devem participar do processo envolvendo-se e comprometendo-se com as metas propostas além de:

- Entender o que é necessário;
- Saber por o que são responsáveis;
- O que é possível com o processo.

O desenvolvimento de uma política de segurança deve ser uma atividade interdepartamental.

As áreas afetadas devem participar do processo envolvendo-se e comprometendo-se com as metas propostas além de:

- Entender o que é necessário;
- Saber por o que são responsáveis;
- O que é possível com o processo.

decriptografarmos dados.

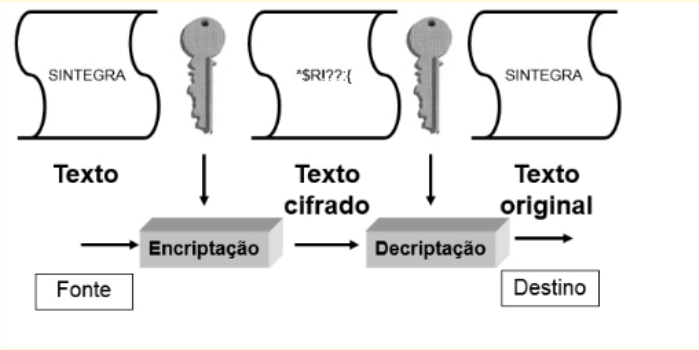
# Mecanismos de segurança

**Ajudam a implementar políticas de segurança e seus serviços:**

- **Criptografia**
- **Filtros**
- **Proxy**
- **Firewall**

# *O que vem a ser a criptografia?*

É a ciência que faz uso da matemática permitindo criptografarmos (cripto=esconder) e decriptografarmos dados.



# Assinatura digital

Mecanismo que pode garantir que uma mensagem assinada só pode ter sido gerada com informações privadas do signatário.

O mecanismo de assinatura digital deve:

A) Assegurar que o receptor possa verificar a identidade declarada pelo transmissor (assinatura);

B) Assegurar que o transmissor não possa mais tarde negar a autoria da mensagem (verificação).

# Firewall

Dispositivo que conecta redes (interna e/ou externa com vários níveis de direito de acesso). Implementa e garante política de segurança entre as redes conectadas.

Quando você conecta sua rede à Internet, é de crítica importância proteger a sua rede contra intrusão. A forma mais efetiva de proteger o link com a Internet é colocar um Sistema de Firewall entre sua rede local e a Internet.

**O que um firewall não faz:**

1) Não protege contra usuários autorizados maliciosos;

2) Não pode proteger contra conexões que não passam através dele;

3) Não fornece 100% de proteção contra todos os THREATS (ataques embutidos no protocolo).

# *O que um firewall não faz:*

1) Não protege contra usuários autorizados maliciosos;

2) Não pode proteger contra conexões que não passam através dele;

3) Não fornece 100% de proteção contra todos os THREATS (ataques embutidos no protocolo).

# Aspectos de Segurança da Informação

Profº Ed W. Jr


Thank you!
Prezi