

# Tecnologias WEB

## Segurança na Web

# Conceitos

- ***E-security*** representa a gestão corporativa da segurança.
- A gestão das informações, pessoas, processos, infra-estrutura, aplicações e tecnologia garantem a segurança dos dados estratégicos, viabilizando a integração entre tecnologia e negócio.

# Conceitos

- Muito do sucesso e popularidade da Internet é por ela ser uma rede global aberta
- Por outro lado, isto faz da Internet um meio não muito seguro
- É difícil identificar com segurança entidades, em um meio sem presença física, face ou voz
- Sendo rede global, a Internet não reconhece limites físicos e jurisdições legais das nações
- Certas situações demandam segurança no tráfego pela Internet

# Conceitos

**Várias abordagens são possíveis para prover segurança no tráfego de dados da Internet**

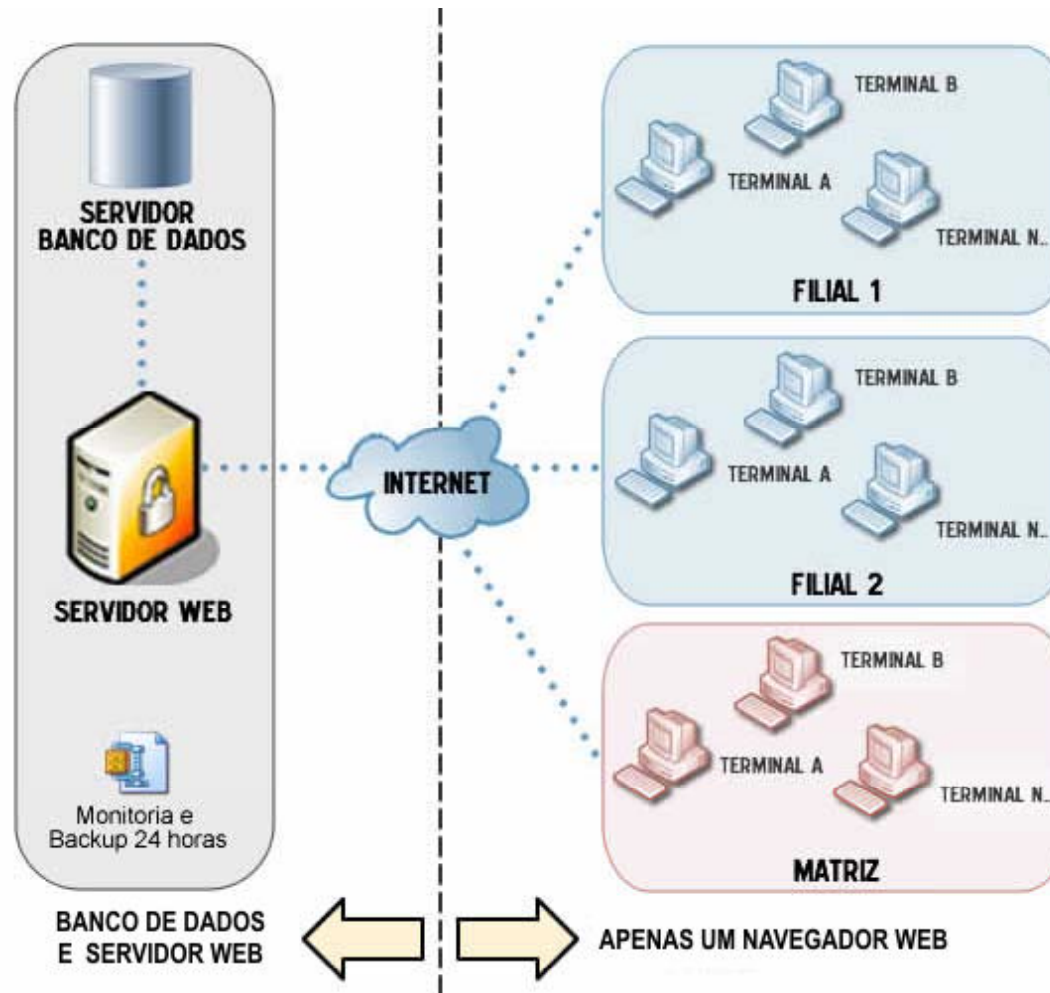
**As opções atualmente existentes provêm serviços e recursos similares, mas variam em escopo e localização na pilha TCP-IP**

# Conceitos

**Uma aplicação web típica está distribuída em vários servidores, rodando diversos aplicativos.**

**Para funcionar na velocidade adequada, necessita que as interfaces entre os sistemas sejam construídas com a premissa que os dados passados através da mesma são confiáveis e não hostis.**

# Conceitos



# Segurança nos Aplicativos

**A segurança dos produtos disponíveis no mercado é assegurada pelos fabricantes, que fornecem periodicamente correções que os atualizam.**

**Para o sistema aplicativo, desenvolvido localmente ou por terceiros, especificamente para uma empresa, não existem correções de segurança.**

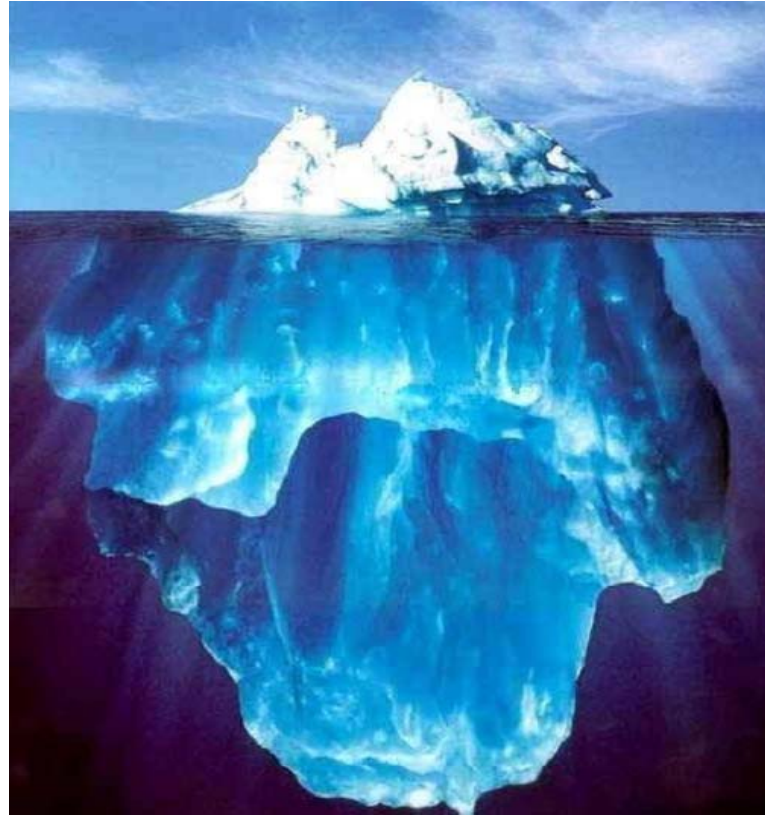
# Vulnerabilidades e Ataques

- **Existem atualmente mais de 4.500 formas conhecidas de ataques que podem atingir os sites de *e-commerce* e de instituições financeiras.**
- **Os ataques mais conhecidos são baseados em vulnerabilidades típicas de aplicações web complexas.**

# Vulnerabilidades

- **A segurança de aplicações, especialmente aquelas conectadas a uma rede aberta como é a Internet é bastante complexa.**
- **A complexidade advém do fato que as aplicações web, e-commerce, Internet banking, na realidade, são agrupamentos heterogêneos de plataformas, bancos de dados, servidores de aplicação, etc..**

# Vulnerabilidades



**A maior parte das vulnerabilidades das aplicações não está visível**

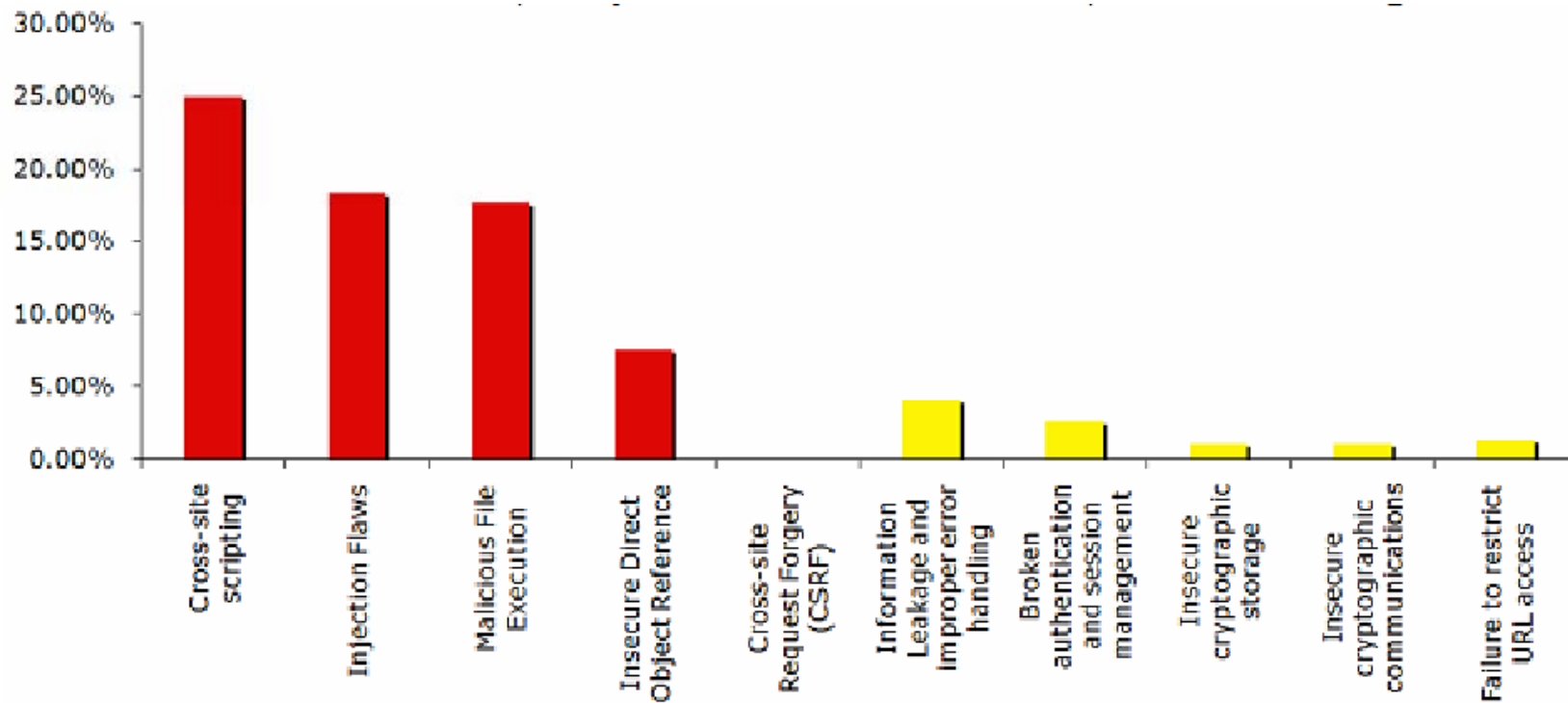
# Ataques

**Os ataques podem causar problemas:**

- **Perdas Financeiras;**
- **Transações Fraudulentas;**
- **Acesso não autorizado aos dados, inclusive informações confidenciais;**
- **Roubo ou modificação de Dados;**
- **Roubo de Informações de Clientes;**
- **Interrupção do Serviço;**
- **Perda da confiança e lealdade dos clientes;**
- **Dano à imagem da marca.**

# Ataques

Aproximadamente 75% dos ataques ocorrem sobre os aplicativos específicos de cada empresa.



# Custo da Segurança

Uma aplicação web típica tem de 150 mil a 250 mil linhas de código. Cada 1.000 linhas de código embutem 15 defeitos de segurança, em média.

Considerando uma aplicação de 200 mil linhas, existirão, portanto, 3.000 defeitos de segurança, que precisarão ser identificados e corrigidos.

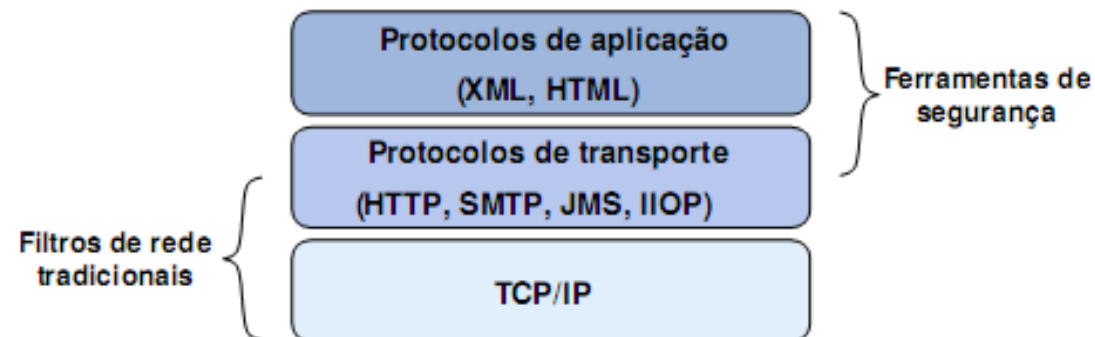
Pode-se estimar o número de horas necessárias para se corrigir todos os defeitos de segurança de uma aplicação típica, supondo-se 5 horas de analista/programador para identificar e corrigir um defeito de segurança:

**200.000 linhas / 1.000 linhas com defeito x 15  
defeitos x 5 horas = 15.000 horas**

# Segurança na Web

Os Serviços Web estão suscetíveis a alguns tipos de ataques já conhecidos.

Para garantir a segurança neste tipo de ambiente, novos mecanismos de segurança devem ser implantados também nas camadas superiores da pilha TCP/IP e devem operar em conjunto com os mecanismos presentes nas camadas inferiores



# Segurança na Web

**As aplicações baseadas nos Serviços Web devem considerar pontos como a transposição de domínios administrativos e de segurança, o que acarreta preocupações com privacidade, anonimato, evolução das políticas de segurança e principalmente, a interoperabilidade.**

**Muitas propostas são analisadas visando cobrir diversas áreas de segurança e, em conjunto com as especificações de segurança para o padrão XML, estas propostas devem garantir alguns dos requisitos mínimos de segurança necessários para as aplicações web.**

# Segurança na Web 2.0

**Segundo o relatório da empresa Websense, publicado no segundo semestre de 2009:**

- **Dos 100 sites mais visitados na Internet, a maioria são redes sociais ou sites de busca.**
- **Quase metade, ou mais de 47%, possuem funcionalidades que dependem do conteúdo gerado pelos usuários.**

# Segurança na Web 2.0

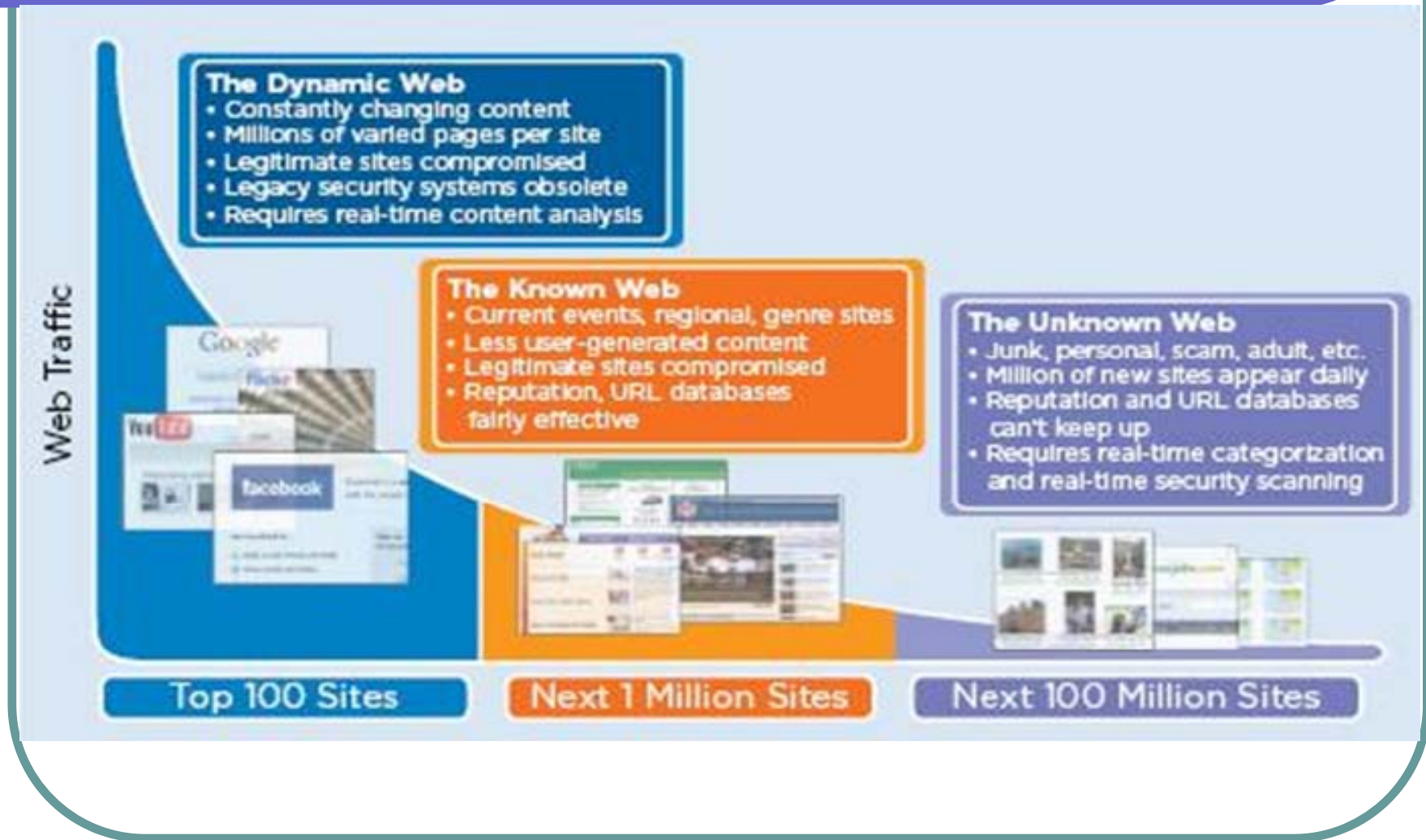
- Ao mesmo tempo, os sites que permitem conteúdo gerado pelo usuário compõem a maioria dos 50 principais e mais ativos distribuidores de algum tipo de *malware*.
- Mais de 60% dos 100 maiores sites da web ou hospedam conteúdo malicioso ou seus usuários apontam links para sites maliciosos sem seu conhecimento.

# Segurança na Web 2.0

**No caso da Web 2.0, observa-se o conflito entre fornecer mais interatividade ao usuário e, simultaneamente, ter-se uma aplicação segura.**

**Ocorrem novas exigências de segurança para as aplicações em função do aumento de tráfego e das novas ameaças**

# Segurança na Web 2.0



# Cuidando da Segurança

**Para obter segurança em uma aplicação para Internet ou Intranet, é preciso cuidar de quatro elementos básicos:**

- ✓ Segurança na estação;**
- ✓ Segurança no meio de transporte;**
- ✓ Segurança no servidor;**
- ✓ Segurança na Rede Interna.**

# Cuidando da Segurança

## **Segurança na Estação**

**Nas aplicações Web, um dos elementos mais vulneráveis é a estação de trabalho, onde normalmente é executado um acesso via browser ou uma aplicação dedicada por onde o usuário tem acesso aos recursos e serviços da rede.**

**Estações de trabalho estão ainda sujeitas a execução de programas desconhecidos (como Applets Java, ActiveX e Javascripts) sendo expostas a grampos e outras armadilhas para obtenção de acesso ilícito.**

# Cuidando da Segurança

## **Segurança no Meio de Transporte**

**Para garantir a privacidade e integridade das informações enviadas pela web, é necessário implementar a segurança no meio de transporte.**

## **Segurança nos Servidores**

**O uso da web exige segurança nos servidores. As empresas têm conectado sua rede interna à Internet, mas não gostariam de conectar a Internet à rede interna. Para isto, torna-se necessário o uso de firewalls que protegem o acesso através de um servidor de controle no ponto único de entrada/saída dos dados.**

# Cuidando da Segurança

## Segurança na Rede Interna

**O desconhecimento técnico da segurança, a ausência do foco e disciplina no assunto, além da ausência da adoção de uma política de segurança consistente serão os principais fatores para o aumento dos riscos na web.**

**A segurança deve prever a proteção e controle da rede interna. O modelo para segurança deve assumir riscos internos e externos, ou seja, os desenvolvedores de sistemas e administradores de rede devem utilizar uma estratégia de controle de acesso externo e interno para os usuários.**



# Obrigado!!

**Prof. José Maurício S. Pinheiro**

**[www.projetoderedes.com.br](http://www.projetoderedes.com.br)**

**[jm.pinheiro@projetoderedes.com.br](mailto:jm.pinheiro@projetoderedes.com.br)**