

PROJETO DE REDES

www.projetoederedes.com.br

Centro Universitário de Volta Redonda - UniFOA
Curso Tecnológico de Redes de Computadores – 5º período
Disciplina: Tecnologia WEB
Professor: José Maurício S. Pinheiro **V. 2009-2**

Aula 6 – Segurança na Web

Dentro da evolução das empresas, o *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 o sucesso na integração entre tecnologia e negócio.

O crescimento do crime na Internet nestes últimos anos deveu-se à crescente profissionalização dos criminosos. De simples *hackers*, para quadrilhas que procuram sistematicamente vulnerabilidades em sites de *e-commerce* e *Internet banking*. As principais vulnerabilidades encontradas costumam ser relativas a erros, acidentes ou desconhecimento dos usuários que, inadvertidamente, alteram configurações de equipamentos, divulgam contas e senhas de acesso, deixam sessões abertas na sua ausência, utilizam senhas fracas ou mesmo contaminam seus arquivos e programas com vírus de computadores.

1. Questões de Segurança

Existem atualmente mais de 4.500 formas conhecidas de ataques que podem atingir os sites de *e-commerce* e de instituições financeiras. Os ataques conhecidos são baseados em vulnerabilidades típicas de aplicações web complexas e tem se concentrado nas portas públicas (80 e 443) que não devem ser bloqueadas pelos *firewalls* comuns, pois os visitantes não acessariam o site, nem as aplicações. Mesmo os *firewalls* mais modernos “*Stateful Multilayer Inspection*” não conseguem analisar e filtrar a camada de Aplicação (camada 7 do modelo OSI).

As aplicações específicas de uma empresa não têm *patches* de atualização e nem foram pensadas em termos de segurança. A segurança das aplicações, principalmente aquelas conectadas a uma rede aberta como é a Internet é bastante complexa (Figura 1). Essa complexidade advém do fato que as aplicações web, *e-commerce*, *Internet banking*, na realidade são agrupamentos bastante heterogêneos de plataformas, bancos de dados, servidores de aplicação, etc..

Uma aplicação típica, geralmente, está distribuída em vários servidores, rodando diversos aplicativos e para funcionar na velocidade adequada, ela necessita que as interfaces entre os diversos sistemas sejam construídas com a premissa que os dados passados através da mesma são confiáveis e não hostis. Não há tempo hábil para duplas verificações. O ponto fraco destas aplicações é a necessidade de haver “confiança” entre os diversos subsistemas e é disso que os hackers e outros criminosos se aproveitam.

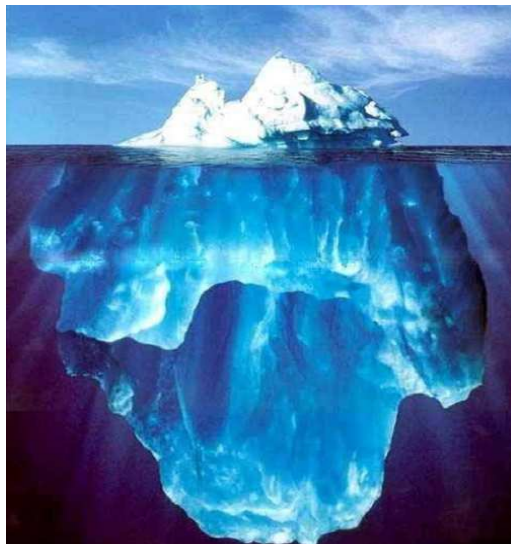


Figura 1 - A maior parte das vulnerabilidades das aplicações não está visível

Os ataques podem causar uma série de problemas, entre os quais se podem citar:

- 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.

A segurança dos produtos disponíveis no mercado é assegurada pelos fabricantes, que fornecem periodicamente correções que os atualizam. Para o sistema aplicativo, freqüentemente desenvolvido localmente ou por terceiros, especificamente para a empresa, não existem correções de segurança.

Segundo recentes pesquisas, aproximadamente 75% dos ataques ocorrem sobre os aplicativos específicos de cada empresa (Figura 2).

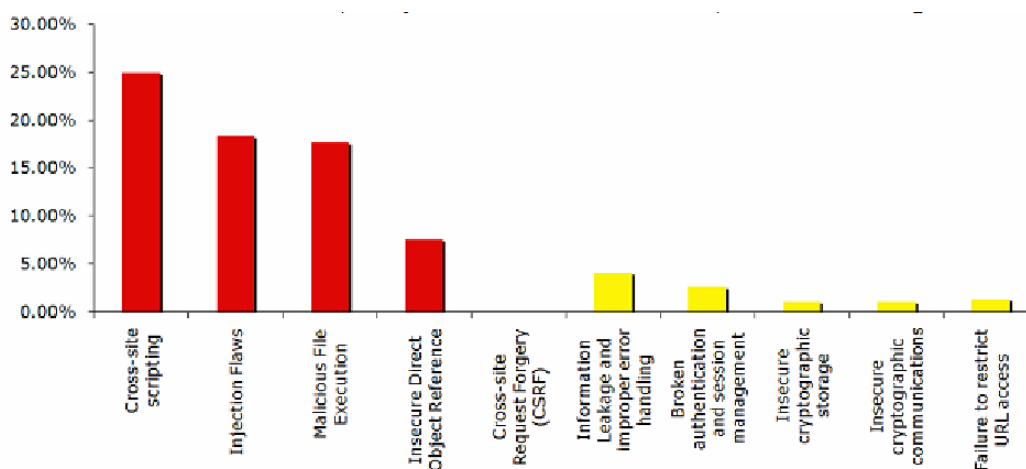


Figura 2 - Vulnerabilidades de aplicações web

Fonte: MITRE – <http://cwe.mitre.org/documents/vun-trends.html>

2. Quanto Custa a Segurança na Web?

Uma aplicação web típica tem de 150 mil a 250 mil linhas de código. Lidam com vários subsistemas, bancos de dados e sistemas operacionais. Na sua especificação são observados normalmente quesitos como rapidez de processamento (os visitantes não gostam de esperar), beleza e usabilidade (a idéia é transformar visitantes em clientes), prazo de entrega e custo baixo.

Normalmente segurança não faz parte dos requisitos do sistema e quanto existe, não se prevê nenhum mecanismo periódico de atualização em função de novas ameaças. Normalmente, a segurança é subentendida como um problema do pessoal da segurança, da infraestrutura e não do pessoal de desenvolvimento ou produto, a não ser em termos de generalidades.

Softwares que analisam aplicações são de grande ajuda para garantir a qualidade em termos de segurança. O que esses softwares não fazem é corrigir a parte defeituosa identificada no código. Isto deve ser feito por analistas e programadores que conheçam o sistema, tenham sido treinados em segurança e sigam uma metodologia que garanta o desenvolvimento de aplicações seguras.

Considerando os estudos na área, cada 1.000 linhas de código embutem 15 defeitos de segurança. Considerando uma aplicação de 200 mil linhas, existirão, portanto, 3.000 defeitos de segurança, que precisarão ser identificados e corrigidos. Um estudo de cinco anos, realizado pelo Pentágono, nos Estados Unidos, estima que se gastem 75 minutos em média para identificar um defeito de segurança e de 2 a 9 horas para corrigi-lo. Pode-se estimar facilmente 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 por defeito x 15 defeitos x 5 horas = 15.000 horas

Cada aplicação demandaria 15 mil homens / hora de analista / programador para ser corrigida. Supondo que cada analista / programador trabalhe 6 horas por dia, vezes 22 dias úteis, são 132 horas de trabalho por mês, ou seja, a aplicação demandaria 114 homens / mês, e se fossem alocados 4 pessoas na equipe de correção, o sistema estaria pronto e corrigido em 29 meses.

Alem do tempo necessário para corrigir os erros e defeitos, o custo, muitas vezes escondido na forma de custos fixos, passa a ser um desafio importante. Tudo isso supondo que a aplicação não sofra melhorias e manutenções, que certamente introduzirão novas falhas de segurança.

3. Serviços Web

Os Serviços Web seguem uma Arquitetura Orientada a Serviços (SOA) e as principais características que os tornam uma tecnologia integradora e promissora são:

- Possuem um modelo fracamente acoplado e transparente que garante a interoperabilidade entre os serviços, sem que estes necessitem ter o

conhecimento prévio de quais tecnologias estão presentes em cada lado da comunicação;

- Usam padrões abertos como o HTTP e XML, por exemplo, permitindo que aplicações sejam integradas através de linguagens e protocolos amplamente aceitos;
- Facilitam a composição ou a combinação de diferentes provedores, visando formar serviços mais complexos.

Os Serviços Web estão suscetíveis a alguns tipos de ataques já conhecidos como negação de serviço (DoS), mensagens antigas, estouro de pilha, entre outros. 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 (Figura 3).



Figura 3 - Segurança nas diversas camadas

Além das propriedades básicas de segurança, a concepção de aplicações baseadas nos Serviços Web deve considerar pontos como a transposição de domínios administrativos e de segurança, o que acarreta em preocupações com a privacidade, o anonimato, a evolução das políticas de segurança, e principalmente, a interoperabilidade.

Com o objetivo de tornar seguro o uso dos Serviços Web, muitas propostas estão sendo analisadas visando cobrir diversas áreas de segurança e, em conjunto com as especificações de segurança para o padrão XML, estas propostas permitirão garantir alguns dos requisitos de segurança necessários para as aplicações.

4. Segurança na Web 2.0

Muitas aplicações Web 2.0 têm características e funções similares às de programas tradicionais, que são instalados e executados no computador do usuário. Pesquisas recentes indicam que os atacantes estão concentrando sua atenção nos seus elementos interativos. Aproximadamente 95% dos comentários gerados por usuários em blogs, fóruns e salas de chat representam spam ou contêm links maliciosos.

Do ponto de vista da arquitetura de software, não há diferenças entre uma aplicação Web 2.0 e um aplicação cliente-servidor tradicional. No entanto, diferentemente de aplicações que são executadas em um ambiente controlado, os sites Web 2.0 são executados em um ambiente hostil, onde a segurança e confidencialidade de informações é um fator crítico. Segundo o relatório "State of Internet Security" 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. 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.

A empresa de segurança ainda assinala em sua pesquisa que as ferramentas de segurança, que permitem às pessoas comunicar conteúdo impróprio, são entre 65% e 75% ineficazes para proteger os usuários da Web a partir de conteúdo censurável e riscos de segurança. Durante os seis primeiros meses de 2009, 78% das novas páginas da Web com conteúdo impróprio, como pornografia ou jogos de azar, continham pelo menos um link malicioso.

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 (Figura 4).



Figura 4 - Evolução do tráfego na Web

5. Ameaças e Vulnerabilidades

Para obter segurança em uma aplicação para Internet ou Intranet, é preciso cuidar de quatro elementos básicos: segurança na estação (cliente), segurança no meio de transporte, segurança no servidor, segurança na Rede Interna.

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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.