*In*Sight

12 de Julho de 2002

Testes Automatizados descobrem vulnerabilidades nas Aplicações Web e impedem ataques de hackers

Se tivéssemos que escolher um único fenômeno relacionado à segurança das informações, que conseguiu acompanhar a enxurrada de novas aplicações web, foi o crescimento do número e da qualificação dos hackers. As ferramentas até agora falharam em proteger as empresas de invasões na camada de aplicações. As soluções de ponta focam na detecção e barramento dos ataques. É necessária uma ferramenta que detecte e remova as inúmeras vulnerabilidades que os hackers podem explorar. Ao invés de tentar parar os ataques dos hackers, testes automatizados detectam as vulnerabilidades das aplicações web e as removem.

Aplicações Web: o coração da empresa

Executivos de visão entendem a presença de suas empresas na web como uma ferramenta poderosa para atingir seus objetivos mercadológicos e um componente crítico da sua identidade empresarial. Quando os sites funcionam como o planejado, clientes, parceiros, acionistas e empregados se beneficiam.

Alvos atrativos para Hackers

Na verdade, web sites e aplicações web são continuamente investigados e atacados com uma facilidade assustadora. Quando um site ou aplicação web são atacados, clientes, parceiros, acionistas e empregados perdem.

A questão não é se, mas quando, a empresa estará na berlinda de hackers bem preparados e mal intencionados. Além disso, será que a empresa conseguirá perceber seu infortúnio?

Infelizmente, mesmo empresas com vasta experiência no desenvolvimento e implementação de aplicações web estão vulneráveis a esforços para sabotar sua presença na rede mundial. Os resultados de uma sabotagem podem causar:

- Perda de informações importantes
- Alterações em informações críticas
- Ficar fora do ar e causar constrangimento público

Raízes do Problema

Diferentemente de muitos problemas baseados na tecnologia, vulnerabilidade em um web site é um problema recorrente, sem uma solução simples. Muitos desenvolvedores que projetam e constroem sites e aplicações web não estão a par de questões de segurança, deixando assim rastros de vulnerabilidades conhecidas, tornando o produto final suscetível a ataques. Ferramentas de desenvolvimento de aplicações comumente utilizadas, como ColdFusion e WebSphere, tornam o problema ainda maior, por deixarem para trás fragmentos que contêm informações úteis aos hackers.

De Mal a Pior

A magnitude do problema dentro da empresa e do mundo web não demonstra sinais de melhora no médio prazo. Aplicações que rodam ou suportam os negócios estão sendo implementadas em números cada vez maiores, e as aplicações estão sempre sendo atualizadas e reconstruídas.

Mesmo os desenvolvedores experientes, deixam traços de vulnerabilidades e não há um esforço muito grande para educá-los na construção de aplicações seguras. Apesar de alguns desenvolvedores estarem melhorando seus conhecimentos sobre segurança, esses mesmos desenvolvedores podem comprovar o ditado “um pouco de conhecimento pode ser uma coisa

perigosa". Uma abordagem errônea sobre segurança de aplicativos deixará a empresa perigosamente exposta.

Combatendo o Problema

Tomadores de decisão da área de TI normalmente utilizam um ou mais produtos reativos para proteger os web sites e aplicações da empresa. A lista pode incluir Sistemas de Detecção de Intrusão (IDS's), Firewalls, ou uma combinação de ambos.

IDS's:

Produtos de IDS baseados em rede capturam pacotes de ataques conhecidos, mas irão falhar miseravelmente em pacotes aparentemente inofensivos, que exploram vulnerabilidades das aplicações. IDS's baseados em host podem ser reconfigurados para detectar uma maior porção de tentativas de ataques, mas devem ser reconfigurados a cada mínima alteração da aplicação, a um custo significativo para a empresa. Além, disso, IDS's baseados em rede ou host foram desenhados para alertar – mas não interromper – tráfego suspeito.

Hackers se escondem dos Firewalls

Usando as portas 80 e 443 como vias expressas através dos firewalls, os hackers estão livres para investigar e penetrar aplicações. Configurados para permitir tal tráfego, os firewalls de rede são incapazes de diferenciar um usuário comum de um hacker. Firewalls de nível de aplicações permitem aos tomadores de decisão da área de TI maior flexibilidade na criação de regras, aumentando marginalmente a segurança das aplicações. Porém, ainda estão limitados ao combate a vulnerabilidades conhecidas.

Proteção Parcial Não é Suficiente

Todos esses produtos, incluindo os firewalls de nível de aplicação, tentam prevenir a exploração de vulnerabilidades conhecidas em aplicações e conteúdo. Nenhuma delas foca na eliminação dessas vulnerabilidades. Projetadas para implementação rápida, uma vez que essas aplicações, vulneráveis, são construídas e postas no ar, esses produtos reativos se tornam escravos de um problema, e não a solução. Estes produtos não conseguirão barrar um hacker habilidoso, que faz investigações cuidadosas, e explora as vulnerabilidades de forma invisível.

Abordagem Proativa

Focar diretamente nas aplicações e estrutura do web site é uma postura mais proativa, mas requer treinamento intensivo para os desenvolvedores. Infelizmente, falta de tempo e disciplina, impedem este tipo de abordagem, na maioria das empresas.

Proteção Parcial = Falha

Ambas abordagens, reativa e proativa, irão falhar perante novas vulnerabilidades e hackers habilidosos. Simplificação excessiva é uma razão – um grupo de regras ou políticas simples que têm como objetivo proteger uma aplicação genérica ou um web site irão inevitavelmente, apesar de não intencionalmente, permitir comportamento inapropriado, que pode levar a intrusões. Além disso, estas abordagens ignoram a melhor defesa contra ataques – estrutura e códigos de aplicações melhorados.
A abordagem reativa não diz aos desenvolvedores de conteúdo e aplicações se o código que está sendo desenvolvido está melhor ou não, sob a ótica da segurança.

Outra abordagem: Verificações Automatizadas das Vulnerabilidades nas Aplicações Web.

Um grama de prevenção equivale a um quilo de cura. Verificações automatizadas das aplicações web, em busca de vulnerabilidades, são o uma grama de prevenção, dando aos desenvolvedores a ótica do hacker para a segurança de seu conteúdo.
A tecnologia incorpora um processo meticuloso de criação de um perfil do conteúdo web alvo, e examina todas suas possíveis entradas. Testes automatizados revelam exatamente como um hacker poderia comprometer o web site ou aplicações de uma empresa. Este processo dá ao pessoal de Segurança de Informação, medidas que os ajudam a melhorar o código no decorrer do tempo.

Além disso, testes automatizados de vulnerabilidades, protegem a empresa de exposições que acontecem apenas pelo fato de que novos métodos de invasão são inventados, mesmo que o código da aplicação não seja mudado. Hoje

uma aplicação aparentemente segura pode virar um prato cheio para hackers inovadores.

Exemplo: WebInspect da SPI Dynamics

O WebInspect é um exemplo claro de verificador de vulnerabilidades em aplicações web. Foi construído especificamente para varrer as aplicações e o web site inteiro, para montar um perfil do conteúdo e seguir os possíveis caminhos que um hacker seguiria.
O WebInspect incorpora um grande conhecimento das técnicas de invasão, que são atualizados automaticamente com o fabricante assim que novas vulnerabilidades são descobertas, via Internet.
Os resultados da varredura e investigação são entregues ao usuário em um relatório completo, que descreve cada vulnerabilidade encontrada e faz sugestões para sanar o problema. O relatório ainda categoriza as vulnerabilidades, baseado no risco que elas representam para a empresa.
Até desenvolvedores que estão destreinados em segurança, podem fazer bom uso do WebInspect, utilizando-o em códigos e sites recém criados ou recém melhorados, construindo assim aplicações resistentes a invasões.

Aplicabilidade na Empresa

Verificações automáticas de vulnerabilidades em sites e aplicações web são extremamente importantes, pois as empresas se utilizam dessas ferramentas para facilitar as transações, freqüentemente de alto valor, ou para acessar conteúdo crítico. A invasão dessas aplicações podem causar à empresa grandes perdas financeira, de imagem, de propriedade intelectual, ou de marca. O tempo requerido para testar e remediar as aplicações e sites são um pequeno investimento frente a um alto retorno.
Além do mais, o uso de soluções de verificação de vulnerabilidades, permite à empresa mudar de atitude. De uma postura reativa, passa-se a ter uma proativa, sem ter que arcar com altos custos de contratação de especialistas em segurança, para que façam os testes de invasão, manualmente.

Em equipes de desenvolvimento de aplicações, que utilizam essa tecnologia, os tomadores de decisão de TI podem reeducar seus funcionários a construir ambientes seguros, ainda durante o desenvolvimento, antes que seja posto o código em ambiente de produção.
Soluções de verificação automáticas de vulnerabilidades podem ser implementadas em módulos de software, que podem ser executadas a partir de qualquer lugar da empresa. Não é necessário nenhuma plataforma dedicada. Não é necessário nenhum monitoramento. Os resultados para os responsáveis pela informática, são custos mais baixos de operação, se comparados aos custos de alternativas menos eficientes, considerando implementação inicial e mudanças que porventura possam surgir.

Conclusões da Aberdeen

A dependência crescente das aplicações web que servem seus clientes, fornecedores, parceiros e empregados, leva a uma enorme exposição para invasões na camada de aplicações. Tomadores de decisão de TI têm duas opções para mitigar a exposição.
Eles podem implementar soluções de barreiras reativas, torcendo para que o produto reconheça e consiga fazer distinção entre tráfego "bom" ou "ruim", ou implementar aplicações já livres de vulnerabilidades perigosas.
As soluções com barreiras são o equivalente digital da estática linha Maginot, francesa, que os alemães contornaram na 2.a Guerra Mundial, passando pela Bélgica.
Soluções baseadas em verificações automatizadas de vulnerabilidades são dinâmicas, constantemente atualizadas e focadas em identificar as brechas que os hackers procuram.
Fornecedores de soluções de verificação automática de vulnerabilidades permitem aos desenvolvedores de aplicações implementar e manter aplicações em menos tempo e a um custo menor. Tomadores de decisão de TI deveriam experimentar essas novas soluções dinâmicas, por serem potencialmente a melhor proteção para as aplicações web das empresas.

Eric Hemmendinger

Aberdeen Group
One Boston Place
Boston, MA 02108
www.aberdeen.com
hemmendinger@aberdeen.com