WebViser

Proteção das Aplicações Web

Fator Crítico para o Sucesso das Operações

KinapSys

Sumário

Introdução

Desde sua criação em 1991 por Tim Berners-Lee, a Web cresceu sob vários aspectos, como pode ser verificado comparando-se os recursos de sites de hoje em dia com os recursos de sites de quase vinte anos atrás. Em muitos casos a complexidade resultante é ordens de grandeza maior que a apresentada nos primeiros momentos da história da Web e isso ocorre porque as facilidades atualmente oferecidas por essa tecnologia às instituições e aos usuários também são muito maiores, se comparadas com aquelas oferecidas na década de 1990. O resultado é que um grande número de atividades que eram desempenhadas no "mundo real" foi transferido para dentro das páginas e das aplicações Web.

Com essas facilidades e a resultante complexidade, veio também o aumento de problemas, de perigos e de riscos Por sua vez, esses riscos, que anteriormente originavam-se na rede, isto é, nos protocolos de comunicação, também evoluíram: agora são originados pelas várias aplicações disponíveis na Web. Justamente essas aplicações — cujo objetivo é entregar as facilidades desejadas pelos usuários por meio dos serviços à sua disposição — tornaram-se o alvo principal de uma vasta gama de ameaças à segurança das instituições, de seus clientes e de todos os internautas.

Instituições que baseiam parcial ou totalmente seus negócios na web preocupam-se ao constatar que as ameaças digitais também evoluíram e cresceram em complexidade. Até pouco tempo, bastava o *firewall* que identificasse origens e destinos não autorizados de tráfego; o IDS que identificasse fluxos de comunicação suspeitos mesmo nos processos com origem e destino supostamente legítimos; o *proxy* que evitasse que agentes externos conhecessem algo sobre a estrutura interna da comunicação. Hoje em dia tais elementos não são suficientes para proteger o ambiente de TI de uma instituição das ameaças existentes. Ataques de *cross-site scripting* e de *SQL Injection*, por exemplo, base de inúmeros golpes e invasões via Web, simplesmente não são identificáveis pelas ferramentas tradicionais de proteção ao perímetro de rede, exigindo um enfoque diferente para serem barrados. Mais preocupante ainda é saber que os efeitos desses tipos de ataque podem ser bem mais nocivos para o ambiente das instituições que os subterfúgios de antigamente. Até pouco tempo o vandalismo era a principal preocupação de administradores de rede. Atualmente, porém, o alvo preferencial dos bandidos são as informações da instituição que podem ser roubadas, apagadas ou adulteradas, ampliando os danos sofridos.

Por que Firewalls de Aplicação?

Para os novos problemas inerentes às aplicações baseadas na Web, novas soluções são necessárias, a fim de assegurar o crescimento dos negócios e das operações, cada vez mais automatizados e virtualizados. Tais soluções devem estar disponíveis em regime 24x7 nos *browsers* dos usuários.

A resposta para os novos desafios vem das tecnologias de avaliação de comportamento das próprias aplicações, denominadas de WAF (*Web Application Firewalls*), cujo alcance de avaliação e proteção apresenta-se muito além do atingido pelas ferramentas tradicionais, voltadas para a proteção de redes.

A tecnologia de WAF faz-se necessária em função do processo de desenvolvimento de aplicações Web ainda deixar muito a desejar quanto às questões de segurança. Existem hoje entre 100 e 150 milhões de aplicações Web em funcionamento. Apenas uma pequena porcentagem delas pode ser considerada segura e, ainda assim, não completamente (1). Por outro lado os *hackers*, encontrando cada vez mais dificuldades de penetrar as defesas de rede das instituições que pretendem atacar — em função de 97% delas já utilizarem ferramentas adequadas de proteção nesse nível, tais como *firewalls* e sistemas de detecção de intrusos —, voltam seus esforços para as aplicações, cujo acesso à página inicial é livre ao grande público por meio dos *browsers*. O resultado é que expressivos 60% dos ataques perpetrados hoje em dia são direcionados às aplicações Web (2). Segundo dados coletados no Brasil, esse percentual pode chegar a 75% (3).

O problema assume proporções ainda mais alarmantes se consideramos os valores transacionais globalmente disponibilizados por essas aplicações, na casa das centenas de bilhões de dólares. Tais cifras incentivam os esforços empreendidos por bandidos virtuais, e demandam constante atenção e atitudes proativas por parte das instituições responsáveis por esses valores. O que se afere em relação às perdas é que, em média, cada incidente custa US$6.655.000,00 para ser reparado, ou cerca US$202,00 por registro comprometido. (5)

Em função desses prejuízos e, sobretudo, da necessidade de proteger os usuários, criam-se normas de segurança que devem ser adotadas por segmentos em que a praxe é o tráfego virtual de valores. Basileia 2, Sarbannes Oxley e outras padronizações tratam de normatizar o mercado, fazendo exigências sérias sobre o ambiente e os processos das instituições. Há muito tempo tais exigências transbordaram os estreitos limites da ISO 9000, sendo que a conformidade hoje é mais que um diferencial de mercado: é uma questão de sobrevivência.

As perdas intangíveis também devem ser consideradas nessa avaliação, pois um incidente que comprometa dados de clientes sempre toma proporções que vão além das perdas financeiras mensuráveis. Tome-se, por exemplo, o caso do roubo de informações da TJX anunciado em 2007. Nessa ocasião a empresa teve 450 mil registros de clientes roubados por *hackers*, o que resultou na troca obrigatória de mais de 45 milhões de cartões nos Estados Unidos. O prejuízo com custo de impacto para a marca, perda de clientes existentes e perda de novos clientes, naquele caso foi estimado em um milhão e quatrocentos mil dólares, não considerado aí os custos de ações judiciais e de campanhas de organizações de classe contra a empresa (4).

O incidente da TJX e várias outras fraudes contra estabelecimentos e empresas que aceitam pagamento eletrônico fizeram com que as bandeiras de cartões se unissem e formassem o PCI SSC – *Payment Card Industry Security Standard Council*, que publicou o padrão PC *Data Security Standard*, ao qual todas as empresas da cadeia de valor de pagamentos eletrônicos estão sujeitas. O PCI DSS estabelece normas e práticas que devem ser seguidas por todas as empresas que recebem, trafegam, armazenam e processam transações de meio eletrônico de pagamento. Já há um cronograma em andamento e as empresas que não tomarem as providências necessárias para proteger seu ambiente de TI e comunicação de dados estarão sujeitas a penalizações financeiras pesadas.

Diante desse cenário, uma solução robusta para proteção das aplicações torna-se imprescindível e, no sentido de propiciar a proteção adequada, a tecnologia de *firewall* de aplicação mostra-se a escolha mais eficaz contra as ameaças crescentes.

O Cerne do Problema

As aplicações baseadas na Web surgem como resposta à necessidade de se oferecer serviços aos clientes a um custo baixo e de forma abrangente, permitindo à instituição focar atenção e recursos em seu *core business* e facilitando a interação com todos os *players* da cadeia de valor, em especial com o cliente. Contudo, esta resposta, que hoje é considerada uma "panaceia", traz consigo algumas questões que precisam ser endereçadas para que a estratégia seja bem-sucedida. Pontos importantes tais como a qualidade das aplicações sendo desenvolvidas e a conformidade das mesmas com relação às normas de desenvolvimento (como os vários níveis da norma CMMI, por exemplo) são algumas dessas questões.

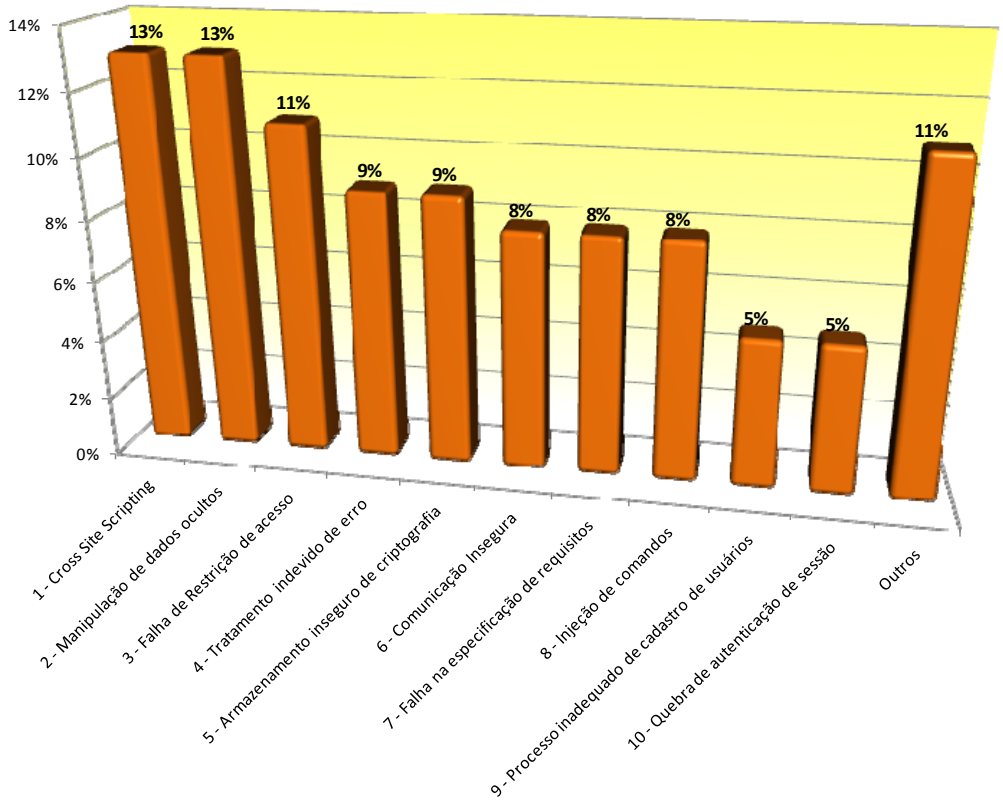
A primeira e a mais crucial questão dentre tantas a ser endereçada, sem dúvida, a segurança. Infelizmente, as aplicações em funcionamento na Web, em sua vasta maioria, não são desenvolvidas tendo a segurança como requisito principal. O resultado é uma coleção de vulnerabilidades que colocam em risco aqueles que utilizam tais aplicações, seja como fornecedores de serviços, ou como clientes dos mesmos. As poucas providências de segurança tomadas durante o processo de desenvolvimento não são eficazes, ou seja, grande parte das vulnerabilidades não é detectada por ferramentas como *scanners* e analisadores de códigos e, quando analisadas, não resultam na devida eficácia (3).

Uma pesquisa realizada pela Kinapsys com empresas atuantes no Brasil resultou na seguinte lista que aponta os principais problemas de segurança encontrados nas aplicações Web (3):

- **1º** - XSS *Cross-Site Scripting* – Técnica de ataque que permite executar *scripts* maliciosos no navegador do usuário da aplicação vulnerável;

- **2º** - Manipulação de dados ocultos – A aplicação vulnerável permite acesso indevido quando dados ocultos são manipulados indevidamente;
- **3º** - Falha ao restringir acesso a URL ou funcionalidade – A aplicação não restringe adequadamente suas áreas restritas;
- **4º** - Tratamento indevido de erro, revelação de informações sensíveis – A aplicação revela informações sensíveis dentro de mensagens de erro geradas pelo uso não esperado da aplicação;
- **5º** - Armazenamento inseguro de criptografia – Dados sensíveis que precisam ser armazenados de forma criptografada estão em texto livre ou com criptografia inadequada;
- **6º** - Comunicação insegura – A aplicação trafega dados sensíveis através de canais não seguros;
- **7º** - Falha da especificação de requisitos – Os controles de segurança que deveriam existir não existem, devido a falhas na especificação;
- **8º** - Injeção de comandos – A aplicação está sujeita a ataques que exploram a injeção de comandos que serão processados por outros sistemas ou camadas. Por exemplo: SQL Injection, SMTP Injection, HTML Injection etc.;
- **9º** - Processo inadequado de cadastro de usuários – O cadastro de usuário deve seguir recomendações rígidas de segurança, que se não forem seguidas podem expor a aplicação a diversos incidentes causados pela falta de segregação adequada dos usuários;
- **10º** Quebra de autenticação e gerenciamento de sessão – Aplicações vulneráveis permitem burlar o processo de autenticação devido a gestão fraca de sessão ou procedimentos inseguros.

Em termos percentuais, temos a seguinte distribuição para esses ataques:



Uma rápida análise qualitativa dessas vulnerabilidades mostra que, se exploradas, as mesmas dariam acesso não autorizado às aplicações, permitiriam o "grampeamento" do fluxo de transação, e a adulteração dos dados das transações. Nenhuma dessas situações é tolerável em um ambiente de missão crítica e qualquer solução que se apresente deve endereçar todas essas questões, não deixando brecha para acesso não autorizado à aplicação, ou ao conteúdo das transações.

Histórico do Cenário de Segurança de Aplicações Web

Quando observamos o cenário de segurança de aplicações Web, não é surpresa encontrarmos paralelos com o desenvolvimento da segurança de redes. No caso dos ataques ao perímetro e aos protocolos de comunicação, encontramos um mecanismo evolutivo no qual a tecnologia foi desenvolvida como reação aos ataques e longo foi o caminho até que o mercado adotasse as soluções criadas, muitas vezes provocando grandes perdas, que acabaram se tornando as principais justificativas – ainda que tardias – para a tomada de ação. Tais soluções, por sua vez, viriam a estimular a criatividade dos ciber-criminosos, que não tardariam a criar novos ataques, forçando sempre a evolução das ferramentas de proteção. Em determinado momento, o próprio

mercado viria a criar conjuntos de melhores práticas e normas para padronizar as soluções. De outro lado, os fabricantes de soluções — navegando em uma região até então desconhecida sob o ponto de vista dos negócios — testariam vários tipos de solução e modelos de negócio, até que o próprio mercado decidisse quais desses trariam valor agregado que justificasse sua existência. A adoção em massa das soluções de proteção de redes surgiria como primeiro resultado dessa maturação do mercado e possibilitaria um ambiente operacional para as instituições, gerando confiança e estabilidade suficientes para a adequada condução dos negócios. Confiança e estabilidade suficientes quando se trata das tecnologias relacionadas a ataques de rede, claro.

Esse ciclo — guardadas as diferenças de geração entre problemas e soluções de uma e outra tecnologia — repete-se com muita similaridade no que diz respeito às tecnologias de proteção às aplicações. Essa similaridade é bastante bem documentada (5), e uma análise de ambos os cenários permite a construção da seguinte tabela:

Segurança de Redes		Segurança de Aplicações	
Ano	**Acontecimento**	**Ano**	**Acontecimento**
1988	Morris Worm, o primeiro vírus de computador distribuído pela Internet, infecta mais de 6.000 máquinas. O incidente propicia as pesquisas que mais tarde resultariam na tecnologia de *firewall* de rede.	**1996**	*Exploit* PHF, uma das mais famosas vulnerabilidades de validação de entrada CGI, é usado para comprometer um grande número de servidores Web. O incidente, junto com outras técnicas de *hacking* existentes na Web, dá início às pesquisas que mais tarde resultariam na tecnologia de *Web Application Firewalls*.
1992	O primeiro pacote comercial de *firewall* baseado em filtro de pacotes (DEC SEAL) debuta no mercado. É comercializado como um dispositivo de segurança de perímetro capaz de impedir ataques remotos visando vulnerabilidades não corrigidas, incluindo o Morris Worm.	**1999**	Os primeiros *Web Application Firewalls* comerciais debutam no mercado. São comercializados como dispositivos perimetrais de segurança de aplicativos capazes de impedir os ataques dirigidos contra vulnerabilidades ainda em aberto, incluindo o *exploit* PHF.
1994 a 1995	Dado que os *firewalls* de rede não são amplamente utilizados e seus custos ainda não estão justificados, os administradores de rede experientes buscam ferramentas para identificar e corrigir vulnerabilidades. É lançado o *ISS*	**2000 a 2001**	Dado que os *Web Application Firewalls* não são amplamente utilizados e seus custos ainda não estão justificados, os profissionais de segurança procuram instrumentos para identificar as vulnerabilidades das aplicações Web. *Scanners*

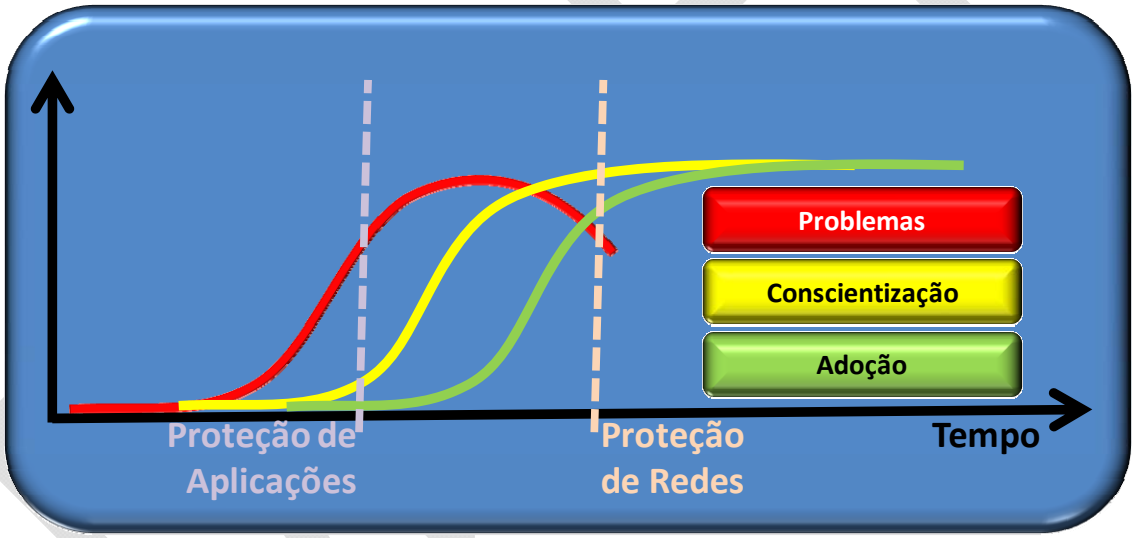
	Internet Scanner, um *scanner* de segurança de rede comercial. A ferramenta *Security Analysis Tool for Auditing Networks* (SATAN) é disponibilizada gratuitamente.		comerciais de aplicativos da Web (AppScan) entram no mercado, bem como versões *open source*, como o Whisker.
1996	Os *scanners* de segurança de rede revelam a necessidade de produtos de gerenciamento de *patches* mais maduros, à medida que as atualizações de segurança se tornam mandatórias com maior frequência. O *PatchLink Update*, um produto comercial de gestão *patches.* Chega ao mercado como uma solução para o problema.	**2001**	Os *scanners* de aplicativos da Web, em conjunto com pesquisas publicadas, revelam a necessidade de mais segurança para os aplicativos da Web. O Projeto Aberto de Segurança para Aplicações Web (OWASP - *Open Web Application Security Project*) é fundado como um esforço da comunidade para melhorar a sensibilização quanto à necessidade de segurança de aplicações Web.
1996	Os custos de software comercial de gerenciamento de *patches* e os períodos de suspensão potencial dos serviços retardam a taxa de adoção da tecnologia. Soluções gratuitas e maduras de gerenciamento de *patch* não existem. Em um ambiente onde poucos sistemas são corrigidos, *hackers* exploram com sucesso grandes números de redes sem defesa.	**2001**	O *Code Red* o *Code Red II* infectam centenas de milhares de servidores Microsoft IIS vulneráveis logo no dia em que são identificados na Internet. O incidente destaca a necessidade de maior adoção do gerenciamento corporativo de *patches*, ainda que somente em *hosts* disponíveis publicamente.
1997	Ataques generalizados destacam a necessidade de controles adicionais de segurança. O software de *firewall* gratuito *Linux IPChains*, torna-se uma alternativa viável aos produtos comerciais. Muitas empresas escolhem *firewalls* de perímetro antes de implantar soluções de gerenciamento de *patches,* porque tais soluções são vistas como alternativas mais rápidas, mais simples e mais eficazes sob o ponto de vista dos custos.	**2002**	Ataques generalizados a aplicativos da Web põem em destaque a necessidade de controles adicionais de segurança. O primeiro *Web Application Firewall* gratuito foi lançado e tornou-se uma alternativa viável aos produtos comerciais. As empresas começam a escolher WAFs antes de adotar iniciativas de software seguro, pois os WAF são vistos como uma abordagem mais rápida, mais simples e mais efetiva sob o ponto de vista dos custos.

1998	Com a ampla disponibilidade de software de varredura de rede (como, por exemplo, o Nessus), a implantação crescente de firewalls, e uma comprovada necessidade de defender a rede contra ataques remotos, cria-se a necessidade de serviços de testes de penetração de rede altamente especializados.	**2004**	Cresce exorbitantemente o número de tipos de ataques e de convenções de nomenclatura de difícil compreensão para leigos e usuários. A lista "OWASP *Top Ten*" é lançada para destacar e descrever as vulnerabilidades de segurança de aplicativos web mais prevalentes e críticas.
1998	Para facilitar o desafio de manter-se atualizado no que se refere aos *patches* de segurança, o Windows *Update* é introduzido no sistema operacional Windows 98.	**2005**	Com a ampla disponibilidade de *software* de varredura de aplicativos Web e outras ferramentas gratuitas, com o aumento na implantação de *Web Application Firewalls*, e com a comprovada necessidade de defender o ambiente contra ataques remotos a aplicações Web, surge a necessidade de serviços de testes de penetração de aplicativos altamente especializados.
2001	O *Code Red* o *Code Red II* infectam centenas de milhares de servidores Microsoft IIS vulneráveis logo no dia em que são identificados na Internet. O incidente destaca a necessidade de uma maior adoção do gerenciamento corporativo de *patches*, ainda que somente em *hosts* disponíveis publicamente.	**2005**	O *worm Samy*, o primeiro *worm XSS* de relevância, infecta mais de 1 milhão de perfis do *MySpace* em menos de 24 horas, causando uma interrupção na maior rede social do mundo até então. O incidente destaca a necessidade de mais segurança para os aplicativos da Web.
2002	Bill Gates lança seu famoso memorando intitulado “Computação Confiável”.	**2007**	Ataques em massa de SQL *Injection* começam a aparecer em bases de dados infectadas por *exploits,* distribuídos via navegação (direto no *browser*). Os visitantes de sites infectados têm suas máquinas comprometidas automaticamente. Este incidente destaca a necessidade de mais segurança para aplicativos Web e do uso de *Web Application Firewalls* para fechar aberturas indevidas nessas aplicações.
2003	O SQL *Slammer* e o *worm Blaster* demonstraram o estado "poroso" da segurança das redes através da	**2008**	Chega ao fim (nos EUA) o prazo estipulado pelo padrão PCI-DSS na seção 6.6, exigindo que os

	exploração de dezenas de milhares de servidores com *patches* desatualizados, mesmo aqueles localizados dentro do perímetro da rede. O incidente destaca a necessidade da adoção de *host-based firewalls* e de implementações de gerenciamento de *patches* para todos os hosts públicos e privados.		comerciantes que aceitam pagamentos eletrônicos realizem revisões de código ou instalem *Web Application Firewalls*. A exigência destaca ainda mais a necessidade de ambas as soluções: comerciais e de código aberto de WAF.
2003	A fim de manter o ritmo com o aumento da frequência de ataques remotos e os requisitos de aplicação de *patches*, cresce a adoção de aplicações *In-House* para a de varredura de vulnerabilidades de rede, para compensar os custos proibitivos dos serviços consultivos de teste de penetração.	**2008 a 2009**	A fim de manter o ritmo com o aumento da frequência de ataques, as aceleradas mudanças nas aplicações Web, e a frequência dos testes de exigidos pela PCI-DSS 6.6, cresce a adoção de aplicações *In-House* para a varredura de vulnerabilidades em aplicações. para compensar o aumento proibitivo nos custos dos serviços consultivos de testes de penetração.
2004	O *Service Pack 2* do Windows XP vem com o *Firewall* do Windows, como um recurso de segurança padrão para proteger os hosts sem correção, que podem ou não estar protegidos por um *firewall* de perímetro. Pouco tempo depois os *firewalls* tornam-se padrão em máquinas conectadas à Internet.	**2008**	Próximos grandes incidentes. Frameworks de desenvolvimento tais como o .NET e o JME adotam mecanismos de proteção contra ataques básicos de aplicações
2005	A ampla adoção das varreduras de vulnerabilidades de rede torna-se realidade, mas os custos de *software* e de gestão são proibitivos. Isso, juntamente com os requisitos de conformidade, leva à maior adoção de serviços gerenciados de segurança e de ofertas no modelo de negócio de SaaS (*software* como serviço), como os exemplos da Qualys e da ScanAlert a fim de reduzir o TCO (custo total de propriedade).	**(?)**	Próximos Incidentes? Ampla adoção de varreduras de vulnerabilidade de rede em regime SaaS?

2006	As bandeiras de cartão de crédito formam o *PCI Security Standards Council*, reforçando a exigência de gerenciamento de vulnerabilidades, gerenciamento de *patches* e ampla adoção de *firewalls*.	(?)	Ampla adoção de *Web Application Firewalls*. Ampla adoção de SDL (*Security Developmet Lifecycle)*, para desenvolvimento seguro de aplicações Web.

O conteúdo da tabela, além de demonstrar com clareza o paralelo sugerido por Grossman, aponta ainda para uma tendência futura de amadurecimento do cenário das aplicações Web e do mercado de *Web Application Firewalls*. Esse amadurecimento é fundamental para que as instituições consigam manter as vantagens da estratégia de soluções via aplicações Web. Em ambos os contextos, tanto de segurança de redes, quanto de segurança de aplicações Web, pode-se deduzir o seguinte gráfico qualitativo:



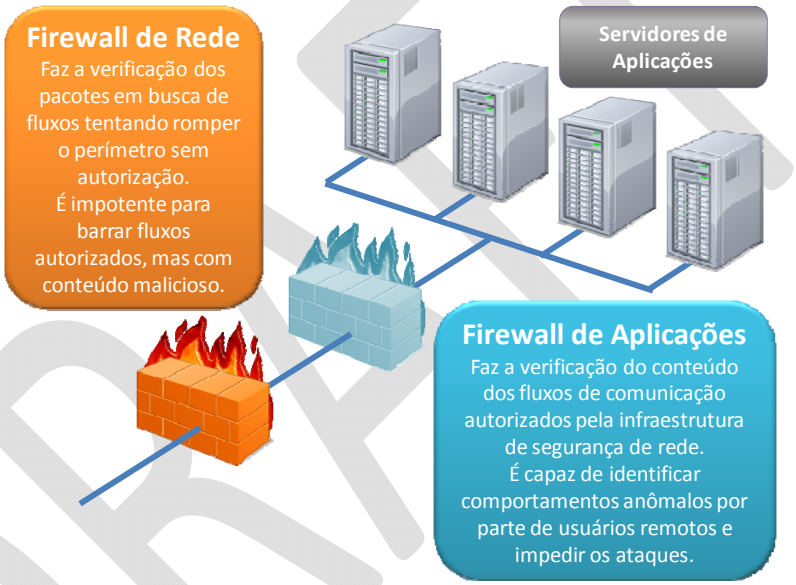
É importante que empresas e internautas compreendam que, enquanto para o cenário de segurança de redes a vasta maioria das instituições já se encontra no platô superior da curva de adoção (verde), no cenário de segurança de aplicações Web ainda nos encontramos na alça ascendente da curva de conscientização (amarelo).

O WebViser da Kinapsys: uma solução efetiva

Com mais da metade dos ataques atuais sendo direcionada às aplicações Web, uma solução que enderece efetivamente esses componentes faz-se imprescindível. O *Web Application Firewall* surge como essa solução.

Mas o que é um *Web Application Firewall*?

O *Web Application Firewall* ou WAF é um elemento de segurança cujo objetivo é proteger os componentes da camada 7 da pilha de comunicação do modelo OSI. Justamente por agir na camada de aplicação, o WAF tem a capacidade de inspecionar o conteúdo do fluxo de informações chegando às aplicações cujo acesso é disponível via Web, determinando se tais fluxos de comunicação são legítimos ou se são maliciosos, isso é, se tentam explorar as aplicações de forma díspar daquela para a qual as mesmas foram criadas. A figura a seguir ilustra o relacionamento e o posicionamento do firewall de aplicações Web dentro da rede da instituição:



Com a intenção de atender às necessidades prementes das instituições, apresentadas anteriormente, e sob o conceito WAF, a Kinapsys disponibiliza sua solução WebViser.

O WebViser é a mais inovadora implantação do conceito de *firewall* de aplicações Web, incorporando as mais novas técnicas de proteção para assegurar o andamento adequado dos fluxos de comunicação com as aplicações baseadas na Web. Dessa forma o WebViser atua oferecendo proteção onde os *firewalls* e demais dispositivos de segurança de rede não conseguem chegar.

As principais características do WebViser são:

- **Ampla proteção para aplicações Web** – O WebViser protege de forma generalizada aplicações cuja comunicação se dê tanto por meio do protocolo HTTP quanto do protocolo HTTPS;
- **Proteção *out-of-the-box*** – O WebViser já em sua instalação inicial, sem que tenham sido feitas customizações específicas, protege contra as vulnerabilidades mais exploradas, melhorando o nível de segurança desde o princípio de sua vida útil na instituição;
- **Modo de Aprendizado** – O WebViser permite a criação de uma base de conhecimento com dados sobre as várias transações possíveis de serem realizadas em uma aplicação Web. Uma vez que essa base tenha informações consolidadas, o WebViser pode ser configurado para reagir adequadamente aos vários tipos de transações coletadas, garantindo maior precisão nas ações e maior efetividade na segurança provida às aplicações;
- **Atualização dinâmica e automática das regras de proteção** – O WebViser disponibiliza um mecanismo automático de atualização das regras de proteção. A equipe de desenvolvimento da Kinapsys está em constante trabalho de pesquisa, identificando novas técnicas de ataque e criando regras para o WebViser que protejam as aplicações desses novos ataques;
- **Gerenciamento Centralizado das Aplicações –** O WebViser disponibiliza uma console centralizada de gerenciamento que permite a visualização dos principais aspectos de utilização e desempenho das aplicações Web sob sua proteção;
- **Geração de Evidências para Análise Forense** – O WebViser gera *logs* que podem ser utilizados para a realização de análises forenses para determinação de causas e atribuição de responsabilidades em incidentes de segurança ocorridos;
- **Auditoria** – O WebViser permite um nível de auditoria nas aplicações inexistente em ferramentas tradicionais de segurança, a exemplo da contabilização e avaliação completa de *posts* e *cookies*;
- **Independência de Plataforma** – O WebViser pode ser implementado para proteger aplicações WEB desenvolvidas em qualquer linguagem e implantadas em qualquer tipo de servidor Web (Apache, IIS, TomCat, Websphere, etc.);
- **Flexibilidade** – O WebViser apresenta grande gama de proteções específicas (boas práticas), e permite também a criação e customização de regras para atender as necessidades críticas de cada cliente e de cada aplicação.

As categorias de proteção do WebViser são:

- **Regras de Filtragem de entrada –** O WebViser permite a implantação de uma ampla gama de regras de filtragem, que protegem contra:
  - *Cross-Site Scripting* (XSS);
  - *Cross-Site Request Forgery* (XSRF);
  - Injeções de comandos em gerenciadores de bases de dados (*SQL Injection*);
  - Comandos incluídos indevidamente nos servidores (*SSI Injection*);

- Comandos nos serviços de autenticação de usuários (*LDAP Injection*);

- **Regras de Filtragem de saída** – O WebViser impede o vazamento de informações por meio de telas e mensagens de erro quando dados incorretos são fornecidos à aplicação. O WebViser intercepta tais mensagens e telas de saída e as substitui por uma tela genérica de erro, sem que o usuário ganhe acesso indevido a informações internas da aplicação. Essas regras permitem ainda a filtragem de determinados padrões, tais como números de cartão de crédito, impedindo que informações sensíveis sejam disponibilizadas indevidamente;
- **Gerenciamento seguro de sessão** – O WebViser introduz novas capacidades ao gerenciamento de sessão, permitindo mais rigor que os controles inerentes às tecnologias das aplicações Web, tais como .Net ou PHP;
- **Filtros extremos (modo positivo)** – apenas um conjunto definido de dados de entrada pode ser passado à aplicação. Quaisquer outras tentativas de entrada de dados fora dos padrões estabelecidos serão automaticamente barradas;
- **Prevenção contra DoS** – Avaliação da freqüência e dos objetivos dos comandos e ações requisitados da aplicação, barrando aquelas cuja intenção seja sobrecarregar a aplicação ou de outra forma debilitar e/ou desabilitar seu funcionamento adequado.
- **Monitoração do seqüenciamento de telas** – Avaliação da seqüência lógica das telas e páginas a serem exibidas pela aplicação. Caso o usuário coloque uma página em "bookmark" para acesso posterior sem precisar passar pelo controle de acesso, essa tentativa falhará;
- **Controle de acesso** – O WebViser pode tomar para si a responsabilidade de controlar o acesso às aplicações Web do cliente, seja por meio de uma base própria de informações dos usuários autorizados, ou por meio da integração com o LDAP da instituição. Por exemplo, o WebViser pode ser integrado com sistemas de autenticação forte, agregando autenticação via *tokens*, biometria e a introdução de certificados digitais para proteção das aplicações Web;

As vantagens da estratégia de proteção de aplicações

O WebViser da Kinapsys oferece uma série de vantagens às instituições clientes, sendo que a principal delas é a consolidação da solução de segurança da instituição. Nesse sentido a adoção de uma estratégia de proteção às aplicações Web complementa e amplia a eficácia da estratégia global de segurança adotada por essas instituições.

Além dessa consolidação — imprescindível ao sucesso nas operações dependentes de aplicações Web da instituição — o WebViser da Kinapsys oferece várias outras vantagens aos seus clientes, a saber:

Foco no Conteúdo

Uma das chaves para o sucesso da estratégia de aplicações Web é o *time to market*. Quanto mais rapidamente a instituição consegue disponibilizar seus serviços na Web, tanto mais rapidamente criará conscientização sobre os mesmos. Tal processo de conscientização é fundamental para tornar realidade os resultados planejados.

A adoção do WebViser permite à instituição focar no conteúdo alvo de sua aplicação sem a necessidade de tempo ou recursos extras que visem à robustez da aplicação. Tais recursos podem ser revertidos para testes de qualidade e melhoria contínua da usabilidade das aplicações, oferecendo valor real aos usuários.

O alicerce dessa estratégia é o WebViser, que abriga em si toda a proteção necessária às aplicações Web, garantindo a segurança dessas aplicações de forma robusta.

A aplicação foi desenvolvida sem foco em segurança? O WebViser evita o retrabalho nas aplicações inserindo-se como a peça de segurança Web na rede.

Novos ataques surgem diariamente na Web? O WebViser dispensa a remodelagem das aplicações para que se adaptem e barrem esses novos ataques. É o WebViser quem vai absorver as novas técnicas de combate e reforçá-las para a instituição.

Os clientes demandam novas características nas aplicações Web? A instituição pode focar seus esforços na implantação dessas características, melhorando a percepção de valor oferecida pelas aplicações.

Evita Retrabalho de Revisão de Código

O Item 6.6 do PCI DSS especifica que as empresas sujeitas ao padrão devem se sujeitar a revisões periódicas (anuais) de código, um processo longo, desgastante e custoso, que pode implicar em paradas, multas e outros custos escondidos, sem contar o efeito negativo para a imagem do estabelecimento ou da empresa em função do tempo de indisponibilidade.

Levando-se em conta que um estudo do Departamento de Defesa dos EUA afirma haver uma média de 15 defeitos de segurança para cada 1000 linhas de código, e que uma aplicação típica tem 200.000 linhas, este processo de revisão de código pode demorar anos para eliminar todos os erros. Muito antes disso, porém, o processo natural de obsolescência fará com que a aplicação seja substituída por outra com outros tantos defeitos, num ciclo vicioso praticamente impossível de ser quebrado.

A adoção do WebViser é uma alternativa aceitável (e recomendável) de acordo com o item 6.6 do padrão PCI, substituindo com vantagens as revisões periódicas de código.

Liberdade das Atividades de Autenticação e Controle de Acesso

O controle de acesso é uma característica crítica das aplicações, exigindo mecanismos de integração com as bases de dados de usuários da instituição e com sistemas tais como o LDAP. Nessas integrações não pode haver falhas. O WebViser oferece mecanismos robustos de controle de acesso que garantem apenas acessos autorizados às aplicações.

Maior Controle Por Meio de Auditoria

A chave para a melhoria contínua da segurança de qualquer ambiente é a monitoração dos eventos que ali ocorrem. O WebViser oferece mecanismos de auditoria muito mais eficientes que os *logs* das aplicações, guardando informações de uso das aplicações para uso forense, quando necessário.

Eliminação de Tráfego Indevido

Elimina tráfego não autorizado, bots, etc., melhorando o desempenho dos recursos de processamento e rede.

Conformidade com Exigências do PCI para 2010

A adoção do WebViser contribui de forma rápida e eficaz para a conformidade com o padrão PCI, cujo prazo para empresas *tier* 1 e *tier* 2 (grande e médio porte de transações eletrônicas anuais) é 31 de julho de 2010. A fim de economizar tempo com o processo de conformidade, a adoção do WebViser de imediato já responde à exigência do item 6.6 do padrão.

Suporte Local

Ao adotar um *firewall* de aplicações Web o cliente introduz em seu ambiente um componente de missão crítica, que como tal precisa ser tratado. Nesse sentido, a agilidade no suporte é uma das questões fundamentais. O WebViser da Kinapsys conta com o suporte de um time local altamente preparado para lidar com as questões urgentes propostas pelos clientes.

Esta equipe garante o mínimo de impacto quando da necessidade de atuação sobre o sistema e o máximo de disponibilidade para as aplicações Web dos clientes.

Conclusão

O cenário global apresentado aponta para um ambiente em constante mutação. Nessas últimas duas décadas houve uma inimaginável evolução tanto no que diz respeito à complexidade da infraestrutura de TI e das informações trocadas on-line, quanto no que concerne às ameaças a essa infraestrutura. O que fica claro é que essas novas ameaças não podem ser combatidas eficazmente com as ferramentas tradicionais.

A adoção de ferramentas de proteção às aplicações torna-se imprescindível à medida que cresce o valor das informações disponibilizadas via aplicações Web, e os firewalls de camada 7 da ISO apresentam-se como soluções para essa questão.

O WebViser representa o estado da arte em proteção de aplicações Web, agindo como barreira contra todas as ameaças — das mais antigas às mais recentes — e está pronto para evoluir ainda mais junto com o ambiente crítico das instituições. Dessa forma o foco da instituição volta a ser a geração de valor para os usuários das aplicações, com a proteção ficando a cargo de quem mais entende do assunto: a Kinapsys.

Próximos passos

Entre em contato com a Kinapsys e participe do programa "*WebViser Case* ". Você pode verificar em primeira mão os benefícios do WebViser, protegendo suas aplicações e garantindo o sucesso de sua estratégia na Web.

Estamos prontos para auxiliá-lo a integrar o WebViser em seu ambiente, protegendo suas aplicações desde o início do projeto e demonstrando claramente porque o WebViser é a melhor solução para seu ambiente Web.

Visite www.kinapsys.com.br e solicite versão de demonstração do WebViser. Você verá que integrá-lo ao seu ambiente de aplicações Web é um processo rápido e simples, cujos resultados falarão por si mesmos.

(1) Khera, Mandeep (Cenzic) – Web Application Security Landscape and Trends – http://www.net-security.org/article.php?id=1139
(2) SANS Institute – The Top Security Risks – Biannual Report – http://www.sans.org/top-cyber-security-risks/
(3) Kiyoshi, Ricardo (Batori) – Confira as 10 Principais Vulnerabilidades em Aplicações Web - http://wnews.uol.com.br/site/noticias/materia.php?id_secao=4&id_conteudo=10324
(4) Singel, Ryan (Wired) – Data Breach Will Cost TJX $1.7Billion, Security Firm Estimates – http://www.wired.com/threatlevel/2007/03/data_breach_wil/
(5) Ponemon Institute – 2009 Annual Study: Cost of a Data Breach – http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf
(6) Grossman, Jeremiah (WhiteHat Security) – History Repeating Itself – http://jeremiahgrossman.blogspot.com/2008/12/history-repeating-itself.html

Para mais informações:
www.kinapsys.com.br
ricardo.batori@kinapsys.com.br
Fone: +55 11 5070-8585