



Documento da F5

Cumprindo as exigências 6.6 do PCI DSS

Em abril de 2008, o Conselho de Padrões de Segurança (SSC, na sigla em inglês) do Setor de Cartões de Pagamento (PCI, na sigla em inglês) publicou um esclarecimento sobre as exigências 6.6 do PCI DSS e forneceu duas opções para as empresas se manterem em conformidade com os padrões. O prazo final para que as exigências 6.6 sejam cumpridas continua sendo 30 de junho de 2008 e, com os esclarecimentos publicados, as empresas têm informações e opções suficientes para desenvolver uma estratégia consistente para a conformidade. Esse documento examinará os esclarecimentos do PCI SSC e sugerirá os modos mais eficientes e confiáveis de atingi-los.

por **Michael Koyfman**

Engenheiro Sênior de Sistema



Índice

Introdução	3
<hr/>	
Exigências 6.6	3
Opção 1 – Revisão do código da aplicação	3
Opção 2 – Firewall de aplicação web	5
<hr/>	
Conclusão	7



Introdução

Em abril de 2008, o Conselho de Padrões de Segurança (SSC, na sigla em inglês) do Setor de Cartões de Pagamento (PCI, na sigla em inglês) publicou um esclarecimento sobre as exigências 6.6 do PCI DSS e forneceu duas opções para as empresas se manterem em conformidade com os padrões. O prazo final para que as exigências 6.6 sejam cumpridas continua sendo 30 de junho de 2008 e, com os esclarecimentos publicados, as empresas têm informações e opções suficientes para desenvolver uma estratégia consistente para a conformidade. Esse documento examinará os esclarecimentos do PCI SSC e sugerirá os modos mais eficientes e confiáveis de atingi-los.

Exigências 6.6

Opção 1 – Revisão do código da aplicação

A opção de revisão do código da aplicação não requer necessariamente uma revisão manual do código-fonte. Tendo em mente que o objetivo das Exigências 6.6 é evitar a exploração de vulnerabilidades comuns (tais como as listadas nas Exigências 6.5), várias soluções possíveis podem ser consideradas. Elas são dinâmicas e proativas, requerendo o início específico de um processo manual ou automático.

Implementada corretamente, uma ou mais destas quatro alternativas podem cumprir com o intento da Opção 1 e fornecer o nível mínimo de proteção contra as ameaças comuns às aplicações web:

1. Revisão manual do código-fonte da aplicação
2. Uso adequado das ferramentas automáticas analisadoras (verificadoras) do código-fonte da aplicação
3. Avaliação manual da vulnerabilidade da segurança da aplicação web
4. Uso adequado das ferramentas automáticas de avaliação (verificadoras) da vulnerabilidade da segurança da aplicação web¹

É importante observar que, independentemente do método escolhido para se atingir a conformidade sob a Opção 1, é preciso resolver todas as vulnerabilidades listadas nas Exigências 6.5. Infelizmente, a revisão manual ou os métodos dos analisadores do código-fonte da aplicação não são suficientemente capazes de identificar os problemas de pelo menos 4 das dez vulnerabilidades listadas nas Exigências 6.5 – incluindo estouros de buffer, reparação incorreta de erros, negação de serviço e gerenciamento inseguro da configuração. Embora tanto a revisão manual quanto os métodos dos analisadores do código-fonte da aplicação possam ajudar a enfrentar essas vulnerabilidades dentro do código-fonte em si, algumas vulnerabilidades estão mais ligadas ao sistema operacional e à versão de configuração do servidor de aplicação/web – algo que tipicamente está além da especialidade ou responsabilidade do desenvolvedor do software. Para lidar com essas vulnerabilidades é preciso realizar uma revisão e uma avaliação do sistema subjacente e de seus componentes participantes.



Uma abordagem mais adequada é utilizar a avaliação manual ou automática da vulnerabilidade da segurança da aplicação web. Como essa avaliação é frequentemente executada em relação ao ambiente de produção, ou tal qual de produção, englobando o sistema operacional subjacente, o software do servidor de aplicação/web, a base de dados e o código da aplicação, é possível realizar testes satisfatórios para as 10 principais vulnerabilidades OWASP ou para as Exigências 6.5.

Há algumas poucas coisas a serem consideradas nesta abordagem. Antes de qualquer coisa, seja no teste manual seja no automático, é preciso que soluções capazes de avaliar os requisitos existentes sejam utilizadas. Essas soluções também precisam ser flexíveis o suficiente para serem ajustadas ou expandidas para cobrir as exigências futuras conforme o PCI DSS for alterado ou atualizado ao longo do tempo. Além disso, é preciso criar, atualizar e executar entradas maliciosas em quantidade suficiente para verificar a conformidade com cada seção do Top 10 do OWASP ou das Exigências 6.5 do PCI. Sem uma ampla experiência e grande especialização, a qualidade das verificações de vulnerabilidade pode não ser suficiente para cumprir com eficiência as exigências do PCI.

As análises/avaliações manuais podem ser realizadas por uma equipe interna ou uma empresa externa desde que qualificadas. Em todos os casos, a equipe precisa ter capacitação e experiência adequadas para compreender o código-fonte e/ou a aplicação web, saber como avaliar cada vulnerabilidade e compreender os resultados.

Se uma equipe interna for ser utilizada, ela deve ser organizacionalmente distinta da equipe de gerenciamento da aplicação que está sendo testada. Por exemplo, a equipe que escreve o software não deve realizar a análise ou avaliação final e verificar se o código é seguro.¹

Isso implica que, se uma equipe qualificada estiver realizando uma análise, ela precisa ter as mesmas habilidades e experiências dos desenvolvedores da aplicação, ser bem versada sobre segurança e pertencer a uma organização interna diferente. Como essa definição também requer um desenvolvedor experiente e com conhecimentos de segurança, o custo de contratar e manter tal indivíduo é bem alto. Além disso, as organizações com apenas um testador qualificado na equipe se arriscam a deixarem brechas na segurança e a atrasarem os ciclos de implementação caso essa pessoa se demita. Se as organizações não conseguirem repor a posição de testador com rapidez, elas podem acabar precisando contar com funcionários temporários, o que encarece a implementação.



Mesmo levando em conta todas as advertências acima mencionadas, atingir a real conformidade por meio da Opção 1 não é um feito insignificante. Há uma desvantagem importante na abordagem da avaliação da proteção em um determinado momento. Esta desvantagem se assenta sobre a premissa de que os testes realizados cobrem 100% das possíveis vulnerabilidades da aplicação. A abordagem restrita a um determinado momento não é capaz de lidar com os ataques emergentes ou com as alterações acidentais nas aplicações ou na infraestrutura que podem ocorrer após a avaliação.

Atingir a conformidade por meio dos métodos da Opção 1 pode implicar em despesas significativas com a aquisição e a manutenção das ferramentas adequadas para a avaliação da vulnerabilidade, com a contratação e o treinamento do pessoal que realizará os testes e em grandes consumos de tempo para gerar os testes capazes de cobrir as áreas comuns de vulnerabilidade para cada aplicação.

Segundo o WhiteHat Security Website Vulnerability Report Snapshot para o primeiro trimestre de 2008, uma análise de mais de 600 sites voltados ao público apontou 4.488 vulnerabilidades não resolvidas, com 9 entre 10 sites apresentando ao menos uma vulnerabilidade importante que impediria a conformidade com o PCI DSS 6.6 e uma média de 7 vulnerabilidades por site (WhiteHat Security, 2008).²

Opção 2 – Firewall de aplicação web

A Opção 2 é uma abordagem que se utiliza de um firewall de aplicação web. Os desafios da implementação da Opção 2 são muito similares aos da Opção 1 – contratar e treinar uma equipe adequada, comprar o firewall de aplicação em si, criar e manter a política de segurança, etc. Entretanto, há alguns benefícios inerentes que tanto reduzem os custos da implementação quanto fornecem um melhor nível de segurança e responsabilização.

É muito mais simples dominar o gerenciamento e o desenvolvimento de políticas de um firewall de aplicação do que realizar as análises da aplicação. Um firewall de aplicação é indiferente à infraestrutura subjacente à aplicação e protege as aplicações escritas em várias linguagens – incluindo Java, C ou PHP. Os firewalls de aplicação focam somente na inspeção do tráfego da aplicação e garantem que as vulnerabilidades da codificação estejam bloqueadas, previnem o vazamento acidental de dados e todas as ações suspeitas são registradas.

Segue uma lista dos recursos de um firewall de aplicação web tal qual descrito na Opção 2 e como eles são apresentados pelo F5® BIG-IP® Application Security Manager™ (ASM):



- Proteção da aplicação contra as vulnerabilidades identificadas nas Exigências 6.5 do PCI DSS e/ou nas Top 10 do OWASP.
- Inspeção das entradas das aplicações web, respostas segundo regras da política e ações registradas.
- Prevenção de vazamento de dados com o recurso BIG-IP ASM DataGuard, que permite bloquear ou mascarar a informação sigilosa proveniente da aplicação, como, por exemplo, números de documentos, de cartão de crédito, etc.
- Reforço dos modelos positivos e negativos de segurança.
- Inspeção tanto do conteúdo da página web (como HTML, DHTML e CSS) quanto dos protocolos subjacentes (HTTP, HTTPS). Validação não apenas do conteúdo, mas também do protocolo subjacente, com garantia da conformidade com os padrões do RFC.
- Inspeção das mensagens dos serviços web, como, por exemplo, as baseadas em SOAP e XML.
- Prevenção contra adulteração da sinalização da sessão.
- Aplicação automática das atualizações dinâmicas da assinatura.

Os benefícios da abordagem com o firewall de aplicação sobrepujam os benefícios obtidos na abordagem da Opção 1. Em particular, um recurso muito útil na abordagem com o firewall de aplicação é o registro. Colocar uma aplicação web em uma rede sem qualquer proteção na frente torna muito difícil julgar quantos ataques são perpetrados contra ela. Também se torna difícil provar aos auditores que a audição do código ou a avaliação da vulnerabilidade são suficientes para cumprir com as Exigências 6.6 do PCI. Em contraste, registros extensos e sumarizados podem ser produzidos pelo firewall de aplicação, particularizando os tipos de ataque defletidos para mostrar a eficácia da política de segurança.

Finalmente, o PCI SSC declara que:

A implementação adequada de ambas as opções deverá fornecer a melhor defesa em múltiplas camadas. O PCI SSC reconhece que os custos e a complexidade operacional de ambas as opções podem não ser viáveis.¹

Os firewalls de aplicação web acrescentam uma camada de defesa possível de ser implementada prontamente ao mesmo tempo em que se realizam avaliações de vulnerabilidade e análise do código-fonte. Isso pode ajudar a corrigir o mais amplamente possível os riscos específicos da aplicação. Inversamente, qualquer método da Opção 1 é capaz de identificar com precisão os riscos, mas as soluções reais geralmente envolvem a correção do código defeituoso ou a paralisação da aplicação enquanto ela é corrigida, o que pode introduzir custos significativos além de atrasos na correção da exposição. Escolher apenas uma dessas duas tecnologias deixa uma lacuna na postura de segurança da organização e muito provavelmente gera custos por ineficiência na eliminação da lacuna.



Entretanto, existem soluções que permitem que as empresas implementem ambas as soluções a um custo eficiente sem que uma grande complexidade operacional seja induzida. Uma empresa pode solicitar serviços especializados na avaliação de vulnerabilidade que se integrem ao fornecedor de um firewall de aplicação e que sejam capazes de alterar imediatamente as políticas para as vulnerabilidades recém-descobertas. A F5, em parceria com a WhiteHat Security, fornece essa solução. O WhiteHat Sentinel, um serviço por assinatura pela web, combina uma avançada tecnologia proprietária de verificação com a análise de especialistas para que os clientes possam identificar, priorizar, gerenciar e corrigir as vulnerabilidades do site no momento em que elas surgirem. O BIG-IP ASM™ fornece uma proteção proativa à rede e às aplicações contra ataques gerais e dirigidos, pois compreende a interação do usuário com a aplicação. Por meio da API do F5 iControl®, o WhiteHat Sentinel é capaz de configurar diretamente as políticas no BIG-IP ASM para proteger contra as explorações das vulnerabilidades (isto é, cross-site scripting, adulteração de parâmetros, injeção de SQL) encontradas no processo de verificação.

Conclusão

Como conclusão, as empresas precisam agir com rapidez e escolher um método de conformidade com as Exigências 6.6 do PCI. A abordagem com o firewall de aplicação web é o modo mais eficiente de proteger as aplicações contra as brechas na segurança e os vazamentos de dados, porque ele bloqueia na fronteira as vulnerabilidades conhecidas ou não e mantém as aplicações e os dados dos clientes em segurança.

1 Security Standards Council. (Fevereiro de 2008)

Informação suplementar: Requirement 6.6 Code Reviews and Application Firewalls Clarified

https://www.pcisecuritystandards.org/pdfs/infosupp_6_6_applicationfirewalls_codereviews.pdf

2 WhiteHat Security. (2008, 1º trim.) WhiteHat Website Security Statistics Report

<http://www.whitehatsec.com/home/assets/WPstats032408.pdf>

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Sede Corporativa
info@f5.com

F5 Networks
Ásia-Pacífico
info.asia@f5.com

F5 Networks Ltd.
Europa/Oriente Médio/África
emeainfo@f5.com

F5 Networks
Brasil
f5networks@f5networks.com.br

