96 – Fevereiro 2008

PCI e o Real Valor do Compliance – parte 2

Quais os impactos da não conformidade?

A não conformidade com o PCI DSS, dada pela falha em demonstrar aderência ao padrão através de implementação de controles de segurança, poderá resultar em multas e outros tipos de penalidades aos varejistas e provedores de serviço. Em uma situação de fraude e comprometimento dos dados de cartão de crédito, a associação de cartões pode cobrar uma multa total de até USD 500.000 e ainda USD 25 por cartão comprometido. Em se tratando de uma cadeia produtiva interligada, a multa poderá ser cascateada até o varejista ou provedor de serviços. Se por sua vez, o varejista ou o provedor de serviço tiver conseguido demonstrar a conformidade com o PSI DSS, realizando os scanners de vulnerabilidade periódicos e ainda tiver passado ileso pela análise forense feita pela associação de cartões depois do incidente, estes podem não estar sujeitos à penalidade, assim como não serem considerados responsáveis pelo incidente.
Em contrapartida, empresas que não tenham sequer um plano para atingir a conformidade ou que tenham criado relatórios inconsistentes de conformidade, estarão sujeitos a penalidades rigorosas.

Como é atribuída a responsabilidade pelo programa de compliance?

A associação de cartões definiu que a responsabilidade por gerenciar os programas de compliance com o PCI DSS fica com as próprias operadoras de cartão de crédito e os bancos emissores. É, portanto, parte de suas responsabilidades, contatar os varejistas, *gateways* de pagamento e provedores de serviço para informá-los sobre seus requerimentos e prazos, quando então deverão demonstrar a conformidade. Varejistas e provedores de serviço são obrigados, por sua vez, a selecionar empresas externas aprovadas e qualificadas como QSA ou *Qualified Security Assessors* pelo próprio *PCI Council*, a executar a avaliação de conformidade e endereçar as medidas corretivas detectadas na avaliação. Neste momento, as operadoras de cartão de crédito podem solicitar planos de ação detalhados para remediar os riscos encontrados. Como é possível notar, há uma estrutura de responsabilidades em cascata, seguindo o modelo de penalidades, que fará com que as ações sejam pulverizadas e supostamente mais eficazes.

Qual é o rigor das rotinas de avaliação de segurança?

O volume de transações é que irá definir o rigor das rotinas de avaliação de segurança requerido dos comerciantes e provedores de serviço. O volume de transações é monitorado pela associação de cartões. Para os comerciantes que consolidam suas operações de pagamento através de *gateways* centralizados, terão seu rigor definido também pelo volume total de transações, sendo obrigados a submeter esses ambientes a rotinas amplas de avaliação de segurança. Em contrapartida, os comerciantes que têm seus ambientes de processamento ligados à rede de cartões, mas não consolidam transações, são classificados apenas como comerciantes coletores. Neste caso, cada um deles terá de completar um

questionário de auto-avaliação e concluir as varreduras de segurança, submetendo os resultados à associação de cartões. Em linhas gerais, existem três categorias de classificação: os que processam mais de seis milhões de cartões anualmente, os que processam entre um e seis milhões de cartões anualmente, e os que processam menos de um milhão de cartões anualmente.
Importante lembrar que tanto para os grandes quanto para os pequenos, seja na condução de rotinas amplas de avaliação de segurança, seja na realização de varreduras, será preciso contratar empresas aprovadas pelo *PCI Council*. As primeiras, chamadas de QSA ou *Qualified Security Assessors*, e as últimas, chamadas de QSV ou *Qualified Scanning Vendors*.

Como começar o planejamento de conformidade?

É comum encontrar interpretações diferentes do PCI DSS quando se compara a visão de gestores distintos, especialmente pela singularidade do ambiente de cada empresa, mas existem ações estratégicas que podem servir a todas e, além de reduzir o risco - o que é unanimemente desejado - podem tornar a tarefa da conformidade menos complexa.

1. Realize uma análise riscos para identificar os perímetros críticos para o PCI;
2. Segregue os ambientes e reduza o escopo do seu sistema de pagamentos;
3. Adote um modelo de gestão de maturidade de controles que os torne mensuráveis;
4. Utilize aplicações em conformidade com o *Payment Application Best Practice*;
5. Atualize e mantenha a política de segurança de acordo com o novo requerimento;
6. Evite armazenar números de cartão de crédito e suas trilhas de dados sensíveis;
7. Adote mecanismos de controle de perímetro;
8. Adote sistemas de controle de acesso, log e integridade de arquivos;
9. Proteja os perímetros de acesso remoto; e
10. Defina um processo específico para manter a conformidade com o PCI.

Conclusões

Sendo crítico, como me é habitual, preciso comentar alguns pontos positivos e negativos da iniciativa PCI. O primeiro e mais negativo deles é o fato de acreditar não ser de responsabilidade exclusiva do comerciante ou do provedor de serviço o ônus pela fragilidade do mecanismo de pagamento que lhe for oferecido, especialmente acreditando já existir instrumentos comerciais e contratuais maduros para regular os riscos inerentes ao pagamento eletrônico. Temo particularmente pelos efeitos colaterais da medida na cadeia produtiva, vendo grandes somas de dinheiro sendo gastas com a conformidade compulsória sem, no entanto, representar ganho de produtividade e retorno direto do investimento.

O segundo e último aspecto negativo está relacionado ao modelo de dependência de empresas credenciadas pela VISA. Parece-me coerente pensar na necessidade de garantir a qualidade dos serviços de conformidade e conseqüentemente, da qualidade do resultado final com base no credenciamento de fornecedores. Entretanto, o modelo de concentração de poder nas mãos de um único agente, o *PCI Council*, pode resultar na criação de um mercado paralelo que venha a ferir, tumultuar ou onerar o legítimo interesse da iniciativa em tornar a experiência do usuário no uso do cartão de crédito, mais confiável e segura.

Mas também existem pontos positivos muito fortes dos quais podemos nos orgulhar. O PCI surgiu de uma iniciativa séria que revisou e considerou diversos padrões de segurança, normas da indústria e regulamentações antes de gerar um conjunto de requerimentos extremamente coerentes e específicos para proteção de dados confidenciais. Com isso, atingiu elevado grau de compreensão por parte dos gestores, o que torna a trajetória de conformidade mais transparente. Além disso, fundiu a visão das principais companhias de cartão de crédito do mundo, fortalecendo as ações de comunicação do projeto e sua reputação. Por fim, a experiência introduzida pelo PCI poderá servir também de referência para outras indústrias no que se refere à proteção de dados confidenciais, além de fomentar o que para os especialistas é o que há de mais valioso no combate à fraude, a cultura de segurança da informação do usuário final.

Marcos Sêmola *é Global IT GRA Compliance Manager da Shell International Limited Gas & Power na Holanda, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information Security Professionals of London. MBA em Tecnologia Aplicada, Professor da FGV com especialização em Negociação e Estratégia pela London School, Bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação, governança e inteligência competitiva. Visite www.semola.com.br ou contate marcos@semola.com.br*

Nota: Este artigo expressa exclusivamente a opinião pessoal do autor, não representando necessariamente a opinião da empresa citada.