OpenPCI: Um toolkit para atender os requisitos técnicos do PCI DSS

Fábio Juliano Dapper, Leonardo Lemes Fagundes

Universidade do Vale do Rio dos Sinos (UNISINOS)
Av. Unisinos, 950 – CEP 93.022-000 – São Leopoldo – RS – Brazil

fjdapper@gmail.com, llemes@unisinos.br

1. Introdução

Com o crescimento da utilização de cartões de crédito e débito, é possível identificar a utilização deste meio de pagamento para a realização de fraudes no comércio varejista e eletrônico. Por exemplo, a invasão dos sistemas que manipulam dados de cartões em empresas como CardSystem (processadora de transações) e TJX (rede de comércio varejista) resultou em um comprometimento de mais de 94 milhões de cartões [Peretti 2008]. É importante salientar que a maioria dos casos envolvendo o comprometimento destes dados nas empresas tem origem na falta de alinhamento com as boas práticas de segurança e com padrões existentes como o *Payment Card Industry Data Security Standard* (PCI DSS) [Novak 2009].

2. Visão geral do toolkit

Este trabalho propõem a criação de um *toolkit* baseado em uma distribuição *GNU/Linux* (*Ubuntu Server*) e que poderá ser utilizado como apoio durante o processo de adequação as exigências do PCI DSS, possuindo como foco principal a implementação de controles técnicos. Considerando o investimento necessário para a aquisição de soluções comerciais, acredita-se que o *OpenPCI Toolkit* seja uma alternativa para se reduzir o custo no processo de conformidade com o PCI DSS.

A estrutura principal do *toolkit* está organizada através de *menus* que correspondem a cada um dos doze requisitos do PCI DSS. Cada *menu* poderá contemplar mais do que uma ferramenta, visto que controles distintos podem ser exigidos em cada requisito. A figura 1 ilustra as principais atividades a serem executadas na utilização do *toolkit*. Tais atividades são descritas conforme a seguir:

- ✓**Atividade 1**: É composta pela execução do SAQ (*Self-Assessment Questionnaire*), um instrumento para análise de aderência com o PCI DSS, que irá retornar ao usuário uma lista de não-conformidades.
- ✓**Atividade 2**: Finalizada a atividade 1, um Relatório de Não-Conformidade (RNC) será apresentado, indicando qual ferramenta disponível no *toolkit* poderá ser utilizada para atender o requisito não-conforme.
- ✓**Atividade 3**: O passo final é a implementação os controles através das ferramentas disponíveis nos *menus* do *toolkit*. A inclusão destas ferramentas no *toolkit* segue critérios como serem livres de custo de aquisição, independente do tipo de licença e atenderem a intenção de cada requisito do PCI DSS.

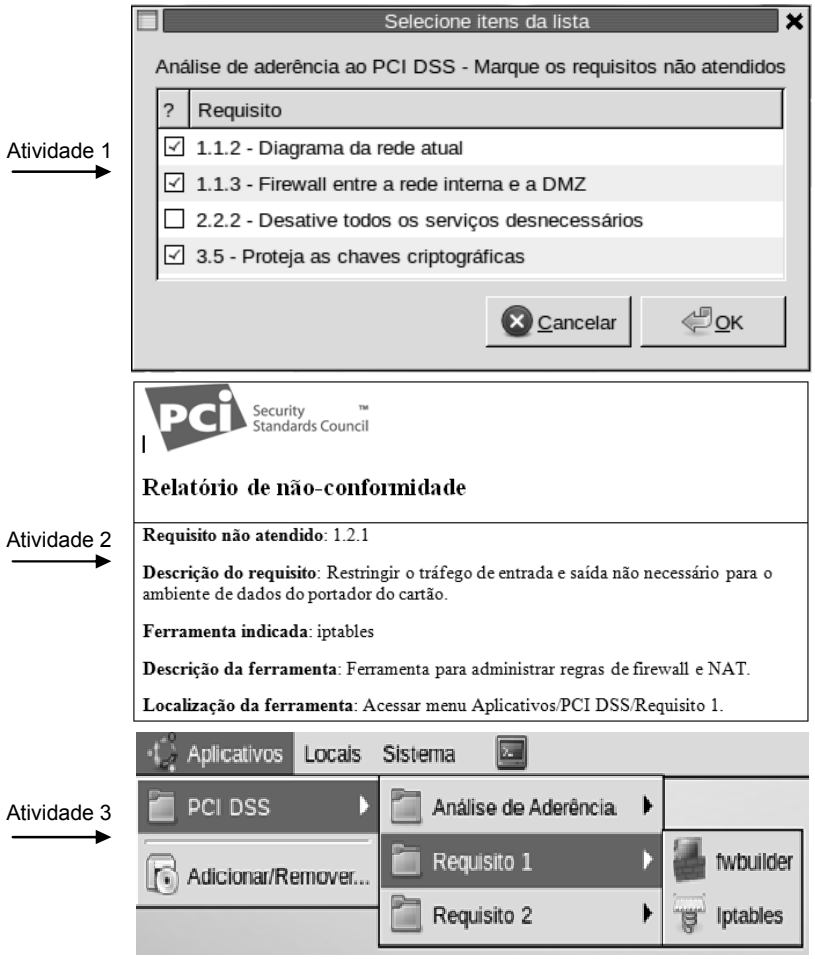

Figura 1. Atividades para utilização do *toolkit*.

3. Conclusão e trabalhos futuros

O processo de conformidade com o PCI DSS pode exigir diversas atividades e entre as principais está a implementação de controles técnicos. Este trabalho pretende contribuir com tal processo através da disponibilização de um instrumento para análise de aderência (SAQ) com o padrão e da organização das ferramentas de acordo com cada requisito técnico exigido.

Para trabalhos futuros, podemos citar uma análise mais aprofundada da intenção de cada requisito, a inclusão de alternativas para cada ferramenta e uma documentação mais detalhada de como tal ferramenta atende o requisito do PCI DSS.

Referências

Peretti, Kimberly Kiefer. (2008) "Data Breaches: What the underground world of "carding" reveals", http://www.cybercrime.gov/DataBreachesArticle.pdf, Agosto.

Novak, Christopher. (2009) "Data Breach Investigations Report", http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf, Agosto.