PCI-NET: Nova Metodologia para Controle da Segurança da Informação na Indústria de Cartões de Pagamento

Ivam G. Wendt, Jeferson L. Prevedello, Rodrigo da Rosa Righi

[1]Universidade do Vale do Rio dos Sinos – São Leopoldo – RS – Brasil.

mail.ivam@gmail.com, jprevedello@unisinos.br, rrighi@unisinos.br

Abstract. *Purchases with payment cards are increasing steadily. This form of payment brings numerous advantages to consumers who do not need to use cash and do not need to be physically in the target store, thus increasing security personnel. Due to the market preference for this form of payment, not accepting it becomes a disadvantage to the merchant. In this context, some companies seek to meet safety requirements proposed by the Payment Card Industry (PCI). Here, we are proposing PCI-NET, a novel methodology for implementation of controls required by PCI DSS environments on computer networks. Thus, PCI-NET can act to help on future implementations that meet these security requirements, which will enable the adoption of the desired certification easier.*

Resumo. *As compras com cartões de pagamento vêm aumentando continuamente. Esta forma de pagamento traz inúmeras vantagens aos consumidores, que não precisam carregar dinheiro em espécie e não precisam estar fisicamente em um estabelecimento, aumentando assim a segurança pessoal. Devido à preferência do mercado por esta forma de pagamento, não aceitá-la torna-se uma desvantagem para o comerciante. Perante este cenário, algumas empresas buscam atender aos requisitos de segurança propostos pela Indústria de Cartões de Pagamento (PCI). O PCI-NET tem por objetivo desenvolver uma metodologia para implementação dos controles exigidos pelo PCI DSS que se apliquem aos ambientes de redes de computadores, auxiliando assim futuras implementações que atendam a estes requisitos de segurança, que possibilitarão o recebimento da certificação desejada.*

1. Introdução

De acordo com a Associação Brasileira das Empresas de Cartões de Crédito e Serviços (ABECS)[1], mais de sete em cada dez brasileiros utilizam cartões de pagamento no consumo de bens ou serviços contribuindo com mais de 60% do total de transações no país [do Brasil 2011]. O comércio eletrônico brasileiro vem crescendo a uma média de 25% ao ano, em 2012 esse comércio movimentou R$ 22,5 bilhões (valor 20% maior que 2011) [camarae.net 2013]. Em 2013, 54% das empresas avaliadas possuíam pelo menos um incidente em potencial de vazamento de informações [Check-Point 2013]. Para organizações financeiras este número foi de 61%. Outro número relevante divulgado foi que, em 36% das organizações financeiras informações de cartão de crédito foram enviadas para fora da organização.

[1]http://www.abecs.org.br/quemsomos

Com o crescente número de incidentes de segurança envolvendo redes de computadores, e com o aumento significativo de transações financeiras realizadas com cartões de pagamento, a demanda por segurança neste tipo de transações é cada vez maior. Em 2004, visualizando o cenário do momento e prevendo o cenário futuro, as grandes operadoras de cartão de crédito (American Express, Discover Financial Services, JCB International, MasterCard e Visa) formaram um conselho com o objetivo de desenvolver um padrão unificado de segurança. Surge então o *Payment Card Industry Security Standards Council* (PCI SSC). Os trabalhos deste conselho deram origem ao *Payment Card Industry Data Security Standard* (PCI DSS) [Barbato 2009].

As empresas que buscam o certificado de conformidade com o PCI DSS precisam implementar controles e tecnologias que atendam aos requisitos de segurança exigidos por este padrão. Neste momento, surgem algumas dúvidas como: *O que deve ser feito em meu ambiente de rede? Como atender aos requisitos impostos pelo PCI DSS? E quanto de meu ambiente está de acordo com o padrão?* Geralmente, empresas de consultoria são procuradas para auxiliar na resposta destas dúvidas. Nesse contexto, o presente artigo tem por objetivo a proposição de uma metodologia chamada PCI-NET, que apresenta uma série de normas e passos que auxiliam os gestores das empresas para atingir as respostas das questões previamente apresentadas. A sua contribuição vai ao encontro da redução de horas necessárias de consultoria e de custos financeiros para a obtenção da normativa.

Este artigo é dividido em seis seções. A seção 2 aborda o PCI DSS e seus requisitos. A seção 3 descreve as atividades propostas pelo trabalho para conformidade do ambiente de redes de computadores. A seção 4 traz os resultados obtidos. A seção 5 discute os trabalhos relacionados com o tema. Por fim, a conclusão do artigo é apresentada na seção 6.

2. PCI DSS (*Payment Card Industry - Data Security Standard*)

O Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI) foi desenvolvido com o intuito de incentivar e aprimorar a segurança dos dados do titular do cartão, independentemente da bandeira, e facilitar a ampla adoção de medidas consistentes de segurança de dados no mundo todo [SSC 2010]. Estas medidas buscam aumentar a Confidencialidade, Integridade e Disponibilidades (CID) das informações.

O PCI DSS oferece a base de requisitos técnicos e operacionais projetados para proteger os dados do titular do cartão onde quer que eles sejam armazenados, processados ou transmitidos. Dentre os doze requisitos do PCI DSS ilustrados na figura 1, cinco deles se destacam por serem relevantes para este artigo: o primeiro ”Instalar e manter uma configuração de *firewall* para proteger os dados do titular do cartão” e o segundo ”Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança” por tratarem diretamente de ambientes de redes de computadores; o quarto ”Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas” por tratar de transmissões de dados do titular do cartão em redes abertas e públicas; o sexto ”Desenvolver e manter sistemas e aplicativos seguros” por tratar da atualização de software dos ativos do escopo do presente artigo;e o décimo ”Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão” por tratar o monitoramento e acompanhamento dos acessos aos recursos da rede.

Os demais requisitos não serão abordados por estarem fora do escopo do presente

artigo, que restringe-se a ambientes de redes de computadores.

Padrão de Segurança de Dados do PCI – Visão Geral Alto Nível

Construir e manter uma rede segura	1. Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão 2. Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança
Proteger os dados do portador do cartão	3. Proteger os dados armazenados do titular do cartão 4. Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas
Manter um programa de gerenciamento de vulnerabilidades	5. Usar e atualizar regularmente o software ou programas antivírus 6. Desenvolver e manter sistemas e aplicativos seguros
Implementar medidas de controle de acesso rigorosas	7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio 8. Atribuir uma identidade exclusiva para cada pessoa que tenha acesso ao computador 9. Restringir o acesso físico aos dados do titular do cartão
Monitorar e testar as redes regularmente	10. Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão 11. Testar regularmente os sistemas e processos de segurança
Manter uma política de segurança de informações	12. Manter uma política que aborde a segurança das informações para todas as equipes.

Figura 1. Visão geral dos doze requisitos do PCI DSS 2.0.

3. PCI-NET: Metodologia para Emprego de PCI DSS no âmbito de Redes de Computadores

Nesta seção serão abordadas as atividades do PCI-NET desenvolvidas para atingir a conformidade do ambiente de Redes de Computadores com o PCI DSS. O PCI-NET foi fundamentado nas informações obtidas no documento ”Navegando pelo PCI DSS: Conhecer a intenção dos requisitos, v2.0”desenvolvido pelo PCI SSC [SSC 2010]. Cada atividade tem por objetivo facilitar o entendimento das ações necessárias para atender aos conjuntos de requisitos específicos da normativa e a visão geral das mesmas pode ser verificada na figura 2.

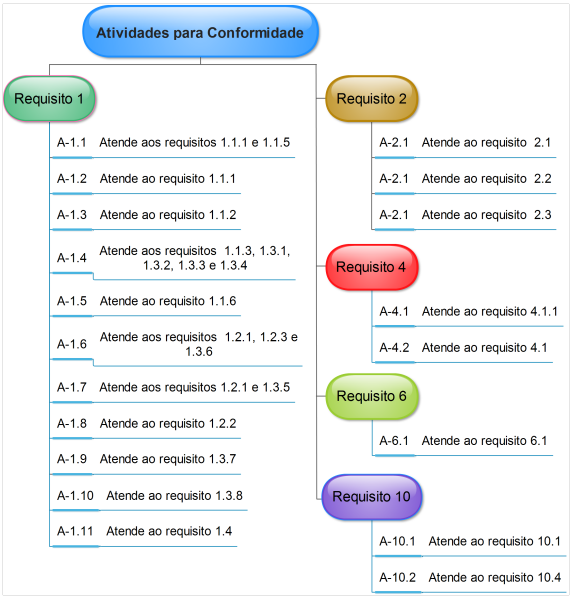

Figura 2. Visão geral das atividades.

- Atividades referentes ao requisito 1: Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão.
  - A-1.1: *Utilizar um documento padrão para solicitações de liberações de Firewall. Atende aos requisitos 1.1.1 e 1.1.5.*
  - A-1.2: *Definir um processo de gestão de mudanças para alterações de firewall. Atende ao requisito 1.1.1.*
  - A-1.3: *Manter topologias/diagramas de rede atualizados. Atende ao requisito 1.1.2.*
  - A-1.4: *Manter uma DMZ. Atende aos requisitos 1.1.3, 1.3.1, 1.3.2, 1.3.3 e 1.3.4.*
  - A-1.5: *Verificar configurações de Firewall e roteadores a cada seis meses. Atende ao requisito 1.1.6.*
  - A-1.6: *Manter firewall statfull entre a rede interna e, redes não confiáveis, redes públicas/abertas e redes sem fio. Atende aos requisitos 1.2.1, 1.2.3 e 1.3.6.*
  - A-1.7: *Manter politica de acessos restritiva, negando todos acessos que não estejam explicitamente permitidos (deny ip any any). Atende aos requisitos 1.2.1 e 1.3.5.*
  - A-1.8: *Sempre salvar a configuração no equipamento após alterações e de preferência (não obrigatório) realizar cópias de segurança das configurações dos equipamentos. Atende ao requisito 1.2.2.*
  - A-1.9: *Implementar os componentes do sistema que armazenam dados do titular do cartão (como banco de dados), na rede interna, fora da DMZ e redes não confiáveis. Atende ao requisito 1.3.7.*
  - A-1.10: *Utilizar na rede interna endereços de IP definidos na RFC 1918. Atende ao requisito 1.3.8.*
  - A-1.11: *Instalar e configurar (não pode permitir alterações por parte do usuário) software de Firewall Pessoal em computadores móveis, que acessam a rede da empresa. Atende ao requisito 1.4.*
- Atividades referentes ao requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança.
  - A-2.1: *Alterar configurações padrões, como: Chave de Criptografia (Wireless), Comunidades SNMP, senhas, e outros padrões ligados a segurança (se aplicável). Atende ao requisito 2.1.*
  - A-2.2: *Desenvolver padrões de configurações para os equipamentos. Removendo todos os recursos desnecessários que estejam sendo executados. (gerenciamento web, telnet, etc.). Atende ao requisito 2.2.*
  - A-2.3: *Para gerenciar equipamento, sempre utilize SSH, ou SSL/TLS (https). Atende ao requisito 2.3.*
- Atividades referentes ao requisito 4: Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas.
  - A-4.1: *Para redes sem fio, utilize as melhores praticas para implementar uma criptografia robusta para a autenticação e a transmissão. (Sugestões: WPA2 com PSK, ou WPA2 com EAP). Atende ao requisito 4.1.1.*
  - A-4.2: *Garanta que a aplicação utilize protocolos robustos de criptografia e de segurança (por exemplo, SSL/TLS, IPSEC, SSH, etc.) para proteger dados confidenciais do titular do cartão durante a transmissão por redes públicas, abertas. Atende ao requisito 4.1.*

- Atividade referente ao requisito 6: Desenvolver e manter sistemas e aplicativos seguros.
  - A-6.1: *Atualizar sistemas operacionais e patches de segurança dos ativos. Atende ao requisito 6.1.*
- Atividades referentes ao requisito 10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão.
  - A-10.1: *Exportar Logs para sistema centralizado, capaz de correlacionar os mesmos. Atende ao requisito 10.1.*
  - A-10.2: *Utilize Network Time Protocol (NTP) para sincronizar os relógios em todos os equipamentos. Atende ao requisito 10.4.*

4. Resultados obtidos

Para verificar a eficácia do PCI-NET, as atividades propostas foram utilizadas no ambiente da Getnet[2], empresa de captura e processamento de transações eletrônicas com cartões de pagamento. Conforme informações obtidas com o Especialista em Telecomunicações João Vitor Duarte Cancelli, a presente metodologia mostrou-se válida e de grande valor durante o processo onde as empresas certificadoras credenciadas (QSAC - *Qualified Security Assessor Company*) recertificaram que o ambiente da empresa esta 100% aderente ao PCI DSS. Segundo o especialista o número de horas necessárias para analise dos requisitos e implementação das atividades foi 50% menor se comparadas com anos anteriores.

5. Trabalhos relacionados

Em [Liu et al. 2010, Dudykevych et al. 2013], os autores exibem os resultados de pesquisas realizadas sobre o PCI DSS e analisam os mecanismos de segurança utilizados pelos sistemas de pagamento. Nestes trabalhos nenhuma metodologia de passos ou documentação foi apresentada. Em adição, Blackwell [Blackwell 2008] investigou o PCI e identificou falhas em seus requisitos em pequenas empresas e propôs algumas regras gerais para a gestão segura de dados on-line. Em [Himmel and Grossman 2014] e [Radford 2014] os autores abordam os desafios e soluções oferecidas para manter a segurança da informações em *cloud computing* e sistemas distribuídos. Por fim, em sua tese de doutorado, Barbato [Barbato 2009] desenvolveu uma metodologia de identificação de vulnerabilidades em aplicações de pagamento utilizando cartões de crédito. O foco do mesmo foi na área de desenvolvimento e aplicações, diferente do foco do presente trabalho que é em rede de computadores.

6. Conclusão

Com a crescente adesão ao comércio eletrônico [camarae.net 2013] e fraudes envolvendo informações de cartões de pagamento [Check-Point 2013], está cada vez mais evidente a necessidade de segurança dos dados do portador do cartão de pagamento em ambientes de telecomunicações. O padrão de segurança PCI DSS busca garantir a segurança destas informações.

Tendo em vista que o PCI-NET busca a conformidade com um padrão de segurança internacional, é possivel afirmar que a comunidade cientifica pode utilizar o

[2]http://www.getnet.com.br/

presente artigo em trabalhos relacionados a este tema. Para trabalhos futuros, sugere-se o desenvolvimento de uma metodologia para avaliação, interpretação e implementação dos controles exigidos pelo PCI DSS que se apliquem a ambientes de Banco de Dados, aplicações de pagamento ou a outros ambientes pertinentes.

Referências

Barbato, L. G. C. (2009). *Metodologia de identificação de vulnerabilidades em aplicações de pagamento utilizando cartões de crédito*. PhD thesis, Doutorado em Computação Aplicada, INPE, São José dos Campos.

Blackwell, C. (2008). The management of online credit card data using the payment card industry data security standard. In *Digital Information Management, 2008. ICDIM 2008. Third International Conference on*, pages 838–843.

camarae.net (2013). E-commerce b2c fatura r$ 22,5 bilhões em 2012. Technical report, Câmara Brasileira de Comércio Eletrônico. Disponível em: <http://www.camara-e.net/2013/03/20/e-commerce-b2c-fatura-r-225-bilhoes-em-2012/>. Acesso em: set. 2014.

Check-Point (2013). Check point 2013 security report. Technical report, Check Point. Disponível em: <http://sc1.checkpoint.com/documents/security-report/files/assets/common/downloads/publication.pdf>. Acesso em: set. 2014.

do Brasil, B. C. (2011). Relatório sobre a indústria de cartões de pagamentos. Technical report. Disponível em: <http://www.bcb.gov.br/htms/spb/Relatorio_Cartoes_Adendo_2010.pdf>. Acesso em: set. 2014.

Dudykevych, V., Bakay, O., and Lakh, Y. (2013). Investigation of payment cards systems information security control. In *Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2013 IEEE 7th International Conference on*, volume 02, pages 651–654.

Himmel, M. A. and Grossman, F. (2014). Security on distributed systems: Cloud security versus traditional it. *IBM J. Res. Dev.*, 58(1):2:3–2:3.

Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S., and Singh, V. (2010). A survey of payment card industry data security standard. *Communications Surveys Tutorials, IEEE*, 12(3):287–303.

Radford, C. (2014). Feature: Challenges and solutions protecting data within amazon web services. *Netw. Secur.*, 2014(6):5–8.

SSC, P. (2010). Requisitos do pci dss e procedimentos da avaliação da segurança, versão 2.0. Technical report. Disponível em: <https://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/minisite/en/docs/pci_dss_v2-0.pdf>. Acesso em: set. 2014.