FONTE: Rede Segura

http://www.redesegura.com.br/gerenciamento-de-vulnerabilidades/recomendacoes-do-pci-dss/

O Payment Card Industry Security Standards Council (PCI-SSC) foi fundado pela American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc., como um fórum global para a disseminação de padrões de segurança na proteção de dados de pagamento, e define o PCI Data Secutity Standart (PCI-DSS).

O PCI Data Secutity Standart (PCI-DSS) especifica recomendações mínimas de segurança obrigatórias para todas as empresas que participam da rede de captura de pagamento com cartões, o comércio, e prestadores de serviços que processam, armazenam e/ou transmitem eletronicamente dados do portador do cartão de crédito.

Os 12 Requerimentos do PCI-DSS

Os 12 requerimentos do PCI-DSS são divididos em 6 seções que visam de modo geral proteger a integridade dos dados de pagamento do usuário do cartão de crédito.

A Metodologia de Segurança recomendada com o uso do Sistema RedeSegura atenderá à vários requerimentos de pelo menos três seções do PCI-DSS. Clique nos títulos a seguir e saiba mais:

Seção: Manter um Programa de Gerenciamento de Vulnerabilidades

Requisito 6: Desenvolver e manter sistemas e aplicativos seguros.

O Sistema RedeSegura permite introduzir critérios de avaliação segurança no ciclo de vida do desenvolvimento das aplicações web, a partir da fase de testes de homologação que avaliam a qualidade da segurança nas entregas do desenvolvedor (Quality Assurance), incluindo os ciclos de melhoria e de atualização dos níveis de segurança.

Os critérios de segurança avaliados pelo Sistema RedeSegura atendem aos requisitos de "scanning" do PCI-DSS para a camada da aplicação web.

O Monitoramento do Risco de ataques pelo ambiente de produção da aplicação web cobre a outra fase do seu ciclo de vida, e mantém atualizado um indicador dos níveis de risco à segurança.

Requerimentos atendidos: 6.6 e 6.5 (6.5.1 até 6.5.9). A Metodologia de uso do Sistema RedeSegura e seus recursos também suportam os demais requerimentos 6.1, 6.2, 6.3, 6.4 e seus subitens.

Seção: Monitorar e Testar as Redes Regularmente

Requisito 11: Testar regularmente os sistemas e processos de segurança.

O Sistema RedeSegura testa estática e dinamicamente todas as recomendações de segurança correspondentes à aplicação web exigidas pelo PCI-DSS, incluindo alguns testes sobre o Sistema Operacional e o Servidor Web (patches de segurança, SSL, e outros). Os testes de vulnerabilidades podem ser feitos externamente ou internamente, tanto no ambiente de desenvolvimento como no de produção, e simulam 39.000 diferentes formas de ataque HTTP a partir de uma base de dados de assinaturas mantida pela tecnologia N-Stalker.

Nossa metodologia de uso permite avaliar continuamente a eficiência dos processos de segurança adotados desde o desenvolvimento. Consulte-nos para saber mais sobre os a cobertura dos testes PCI-DSS do RedeSegura.

Requerimentos atendidos: 11.2 (11.2.1, 11.2.2 como ferramenta do ASV, e 11.2.3). Os recursos do Sistema RedeSegura orientam o processo de "pen test" do requerimento 11.3 (11.3.2).

Seção: Manter uma Política de Segurança das Informações

Recomendação 12: Manter uma política que aborde a segurança das informações.

O Sistema RedeSegura é orientado ao gerenciamento de um processo que monitora os indicadores de vulnerabilidades nas aplicações web, permitindo assim a manutenção de um processo de melhoria contínua da segurança (PDCA).

Este processo estende para a camada da aplicação web o alcance da Política de Segurança da Informação definida pela sua empresa. O processo implementado com a Metodologia de Segurança RedeSegura integrará as equipes técnicas multidisciplinares de segurança da informação, de desenvolvimento, de infraestrutura, de Risco e Compliance, e até a de qualidade, em uma política de segurança mais abrangente e orientada ao PCI-DSS em todo o ciclo de vida das aplicações web.

Requerimentos atendidos: Vários subitens do requisito 12 encontram suporte e documentação na Metodologia de uso do Sistema RedeSegura e seus recursos.

A metodologia de uso do Sistema RedeSegura para o Gerenciamento de Vulnerabilidades permitr manter o nível da segurança da aplicação web em conformidade com os patamares exigidos, mantendo evidências dos testes e indicadores de resultados auditáveis, o que garante o atendimento à estas 3 recomendações do PCI-DSS.

As 6 Categorias	#	Os 12 Requerimentos do PCI-DSS
Construir e Manter uma Rede Segura	1	Instalar e manter uma configuração de firewall para proteger os dados do portador de cartão.
	2	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança.
Proteger os Dados do Portador de Cartão	3	Proteger os dados armazenados do portador de cartão.
	4	Codificar a transmissão dos dados do portador de cartão em redes abertas e públicas.
Manter um Programa de Gerenciamento de Vulnerabilidades	5	Usar e atualizar regularmente o software antivirus.
	6	Desenvolver e manter sistemas e aplicativos seguros.
Implementar Medidas de Controle de Acesso Rigorosas	7	Restringir o acesso aos dados do portador de cartão de acordo com a necessidade de divulgação dos negócios.
	8	Atribuir um ID exclusivo para cada pessoa que tenha acesso a uma computador.
	9	Restringir o acesso fisico aos dados do portador de cartão.
Monitorar e Testar as Redes Regularmente	10	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do CC.
	11	Testar regularmente os sistemas e processos de segurança da informação.
Manter uma Política de Segurança das Informações	12	Manter um política que aborde a segurança das informações.

Auditorias e Formalidades do PCI Compliance

(QSA) O processo de certificação do PCI-DSS (versão 2.0) para empresas (merchants) que movimentam volumes acima de 6 milhões de transações exige um relatório de auditoria "on site" feito por uma empresa credenciada como Entidade Certificadora, definida como**Qualified Security Assessor (QSA)**:

• Auditoria independente que avalia a aderência da empresa a todos os requerimentos de segurança do PCI-DSS

• Analisa a documentação de segurança, relatórios anteriores de "scanning" internos e externos (ASV Report)

• Emite um relatório formal após a avaliação "on-site" (annual report)

(SAQ) As demais empresas que movimentam menos de 6 milhões de transações por ano devem responder um questionário **Self-Assessment Questionnaire (SAQ),** além de contratar trimestralmente um scanning externo:

• Instrumento de validação para empresas que não precisam se certificar através de um QSA (pequenas e médias)

• SAQs diferentes são definidos para cada situação do negócio

Independentemente do volume de transações anuais, é recomendado que a empresa realize trimestralmente pelo menos um teste de avaliação **externo** para identificar vulnerabilidades no seu ambiente de infra-estrutura, assim como sobre a aplicação web, além de testes **internos** regulares que avaliam a segurança de seu ambiente preventivamente.

(ASV) Para os **testes externos** trimestrais a empresa deve contratar o serviço de um **Approved Scanning Vendor**

(ASV), e para os **testes internos** pode utilizar-se de recursos e ferramentas próprias, de terceiros, ou de um ASV:

• O ASV utiliza um conjunto de ferramentas de teste, uma metodologia padrão, e uma equipe técnica com pessoal Certificado pelo PCI para realizar os testes definidos no requerimento 11.2 do PCI-DSS;

• O "scanning" de vulnerabilidade será realizado externamente, via acesso internet ao menos uma vez a cada trimestre. A sua empresa (Scan Customer) deve realizar periodicamente "scans" internos com o mesmo alcance dos testes do ASV.

• Os testes não podem causar impacto, não incluem penetração, e geram um relatório com evidências (ASV Scan Report Attestation of Scan Compliance cover sheet).

O Sistema RedeSegura "powered by" N-Stalker pode integrar a Solução Técnica adotada pelo **ASV e/ou QSA** como parte de seus recursos de avaliação para o **"scanning" externo** e certificação, pois produz as evidências e os relatórios de vulnerabilidades que são exigidos como documentação pelo PCI-DSS.

Adicionalmente, o Sistema RedeSegura pode ser adotado como uma ferramenta poderosa para os testes de **"scanning" internos** da sua empresa, enquanto mantém seu processo de Gerenciamento de Vulnerabilidades.