Por que sua empresa deve proteger os dados de cartão de pagamento através do PCI DSS?

MODULO

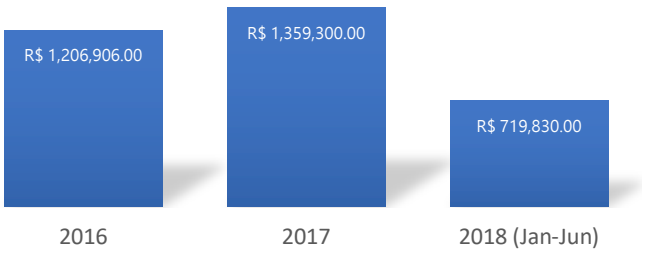
Avenida das Nações Unidas,
12901 – 24º andar, Sala 24.140
São Paulo – SP | CEP: 04578-910

> Uma pesquisa nacional realizada pelo Serviço de Proteção ao Crédito (SPC Brasil) e pela Confederação Nacional de Dirigentes Lojistas (CNDL) revela que 54% dos consumidores brasileiros foram vítimas de algum tipo de fraude nos últimos doze meses.
>
> Fonte: SPC Brasil

Negócios de todos os tamanhos e segmentos lidam diariamente com dados de cartões de pagamento (crédito e débito), segundo o Congresso de Meios Eletrônicos de Pagamentos (CMEP) em 2017 foram realizadas R$ 1,36 trilhões em compras com cartões no Brasil, um crescimento de 12,6% em relação a 2016. Somadas, as transações realizadas com meios eletrônicos de pagamento já representam 32,6% do consumo das famílias brasileiras.

As projeções do setor indicam que o número de transações deve atingir R$ 1,57 trilhão em 2018 – um crescimento entre 14,5% e 16,5% em relação a 2017, segundo projeção da ABECS (Associação Brasileira de Empresas de Cartão de Crédito e Serviços).

Gastos de Brasileiros com Cartões



Porém, proporcional ao crescimento da utilização dos cartões como meio de pagamento, é crescente o número de fraudes originadas de vazamento dos dados de cartão. O vazamento deste tipo de dado tem sido um dos principais alvos de *cyber* ataques no País, de acordo com um estudo recente da Verizon, 78% dos vazamentos de dados envolvem informações de cartão de pagamento.

Um levantamento feito pela Confederação Nacional dos Dirigentes Lojistas (CNDL) e do Serviço de Proteção ao Crédito (SPC Brasil) estima que, em 12 meses até setembro deste ano, 7,8 milhões de brasileiros foram vítimas de fraude. Os dados mostram que a maior parte das ocorrências (41%) está ligada à clonagem de cartão de crédito.

Diante deste cenário, o Conselho de Padrões de Segurança PCI SSC com o seu *framework* global desenvolvido de forma colaborativa por organizações lideres no mercado de pagamento dentre elas Visa, Mastercard, American Express, Discover e JCB, apresenta um framework sintetizado em 12 requisitos, com o objetivo de manter os sistemas e ambientes protegidos.

Os 12 requisitos do PCI DSS .

Construir e manter a segurança de rede e sistemas	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 titular 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. Proteger todos os sistemas contra *malware* e atualizar regularmente programas ou software antivírus 6. Desenvolver e manter sistemas e aplicativos seguros
Implementar medidas rigorosas de controle de acesso	7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio 8. Identificar e autenticar o acesso aos componentes do sistema 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 da informação para todas as equipes

Tabela 1 - Padrão de segurança de dados do PCI – Visão geral alto nível

Todas as empresas envolvidas na transmissão, processamento ou armazenamento de dados de cartão de pagamento, inclusive provedores de serviços terceirizados devem aderir ao PCI DSS (Data Security Standard) de forma contínua, comprovando anualmente a conformidade ao padrão.

A conformidade com o PCI DSS é obrigatória para instituições financeiras, *fintechs*, estabelecimentos comerciais, *gateways* de pagamento, adquirentes, sub-adquirentes, *contact centers*, emissores, agências de turismo, prestadores de serviços e demais empresas que operam dados de cartão de pagamento.

Porque sua empresa deve proteger os dados de cartão através do PCI DSS?

1. Aumento da Credibilidade

Empresas com o certificado PCI DSS têm maior confiança, atraindo mais clientes e consequentemente aumentando as vendas.

2. Maior Rentabilidade

A implementação das melhores práticas de segurança em conformidade com o PCI DSS pode trazer maior rentabilidade, uma vez que seu negócio evita perdas e custos legais relacionados a vazamento de dados de cartões.

3. Redução Expressiva do *ChargeBack*

O *ChargeBack* é uma demanda por parte de um provedor de cartão de crédito para que o vendedor devolva o valor de uma transação fraudulenta ou disputada. A implementação das práticas do PCI DSS evita o vazamento dos dados de cartão de pagamento, que por consequência evita as transações fraudulentas que originam os pedidos de *chargeback*.

Como Podemos Ajudar?

Apoiamos sua empresa no entendimento dos requisitos e conceitos envolvidos para adequação do seu ambiente computacional e dos procedimentos internos, viabilizando alcançar e manter a certificação PCI DSS de forma ágil, levando a sério o tratamento dos riscos de seu ambiente, elevando a maturidade da segurança através da expertise do nosso time de consultores especialistas em segurança cibernética.

A Módulo é a empresa pioneira na proteção de dados de cartão no Brasil, certificada pelo conselho de normas de segurança PCI SSC (*Security Standard Council*) como QSA (*Qualified Security Assessor*). Essa certificação nos habilita a auditar e certificar empresas aderentes ao padrão PCI DSS (*Data Standard Security*).

Para execução dos projetos utilizamos a plataforma digital Módulo Risk Manager™, onde o consultor e o cliente possuem todas as informações e relatórios necessários para o acompanhamento das atividades em todas as fases do projeto em tempo real.

Nossos Números

- Primeira empresa QSA do Brasil;
- Mais de 3 décadas entregando grandes projetos de gestão de riscos dentre eles: eleições eletrônicas brasileiras, imposto de renda via internet, XV Jogos pan-americanos do RJ, Conferência das Nações Unidas Rio + 20; Jornada mundial da Juventude JMJ 2013, Copa do mundo da FIFA 2014;
- Primeira empresa certificada ISO 27001 no mundo.

Nossos Serviços

Auditoria Anual (CVS)

Serviço anual de avaliação de conformidade (CVS) com padrão PCI DSS, através da avaliação dos ambientes que armazenam, processam ou transmitam dados do titular do cartão (CHD) e/ou dados de autenticação confidenciais (SAD). A Módulo é certificada pelo Conselho de Segurança PCI autorizada a realizar avaliação dos sistemas e dos ambientes que estão no escopo citado acima.

Avaliação on-site, análise de desvios (*GAPs*)

Auditoria de avaliação dos controles PCI DSS aplicáveis ao negócio, com objetivo de verificar a aderência da empresa ao padrão e definição do status de conformidade acerca dos requisitos. A análise de *GAPs* possibilita que sua empresa identifique e resolva os problemas antes de uma auditoria anual (CVS).

Consultoria de Correção

Apoiaremos sua equipe de segurança no plano de ação e projeto de correção dos desvios (*GAPs*) encontrados durante a auditoria, independente da análise ter sido realizada pela Módulo ou por outras empresas.

Análise de Vulnerabilidade

Realizamos varreduras com o objetivo de identificar vulnerabilidades de acordo com os critérios definidos pelo PCI. O resultado desta análise identificará todas as vulnerabilidades em seu ambiente.

Teste de Intrusão

Nossos especialistas irão descobrir as fraquezas e vulnerabilidades de seu ambiente através de métodos *ethical hacking*, seguindo os critérios do PCI.

Para conhecer melhor nosso serviço acesse:
pci.modulo.com

Fontes:

https://www.spcbrasil.org.br/pesquisas/pesquisa/5546
http://site.cndl.org.br/spc-brasil-54-dos-consumidores-ja-foram-vitimas-de-fraude/
http://www.cmepabecs.com.br/
https://www.abecs.org.br

A Módulo é uma empresa brasileira, com atuação internacional, especializada em soluções para Governança, Riscos e Compliance. Líder nos segmentos de Segurança da Informação e Gestão de Vulnerabilidades em TI (IT GRC), Gestão de Riscos Operacionais, Gestão de Riscos Corporativos (ERM – Enterprise Risk Management), de Centros Integrados de Operações para Gestão por Indicadores, Cidades Inteligentes e Grandes Eventos.

Copyright © 2018 | Módulo Security Solutions S/A - All Rights Reserved.