PCI-DSS: Entenda como funciona a norma de segurança de transações eletrônicas

Friday, 03/04/2009 às 09h04, por Douglas Falsarella

Nos últimos 10 anos, houve uma explosão de negócios via Internet – e-commerces – na mesma proporção que aumentou o uso de cartões de crédito para compras em estabelecimentos comerciais e, é claro, sites de internet.

Apesar de todos os esforços das empresas de proteger as informações de clientes, fraudes eletrônicas e roubos de informações têm aumentado drasticamente. Em 2006, mais de US$ 4 milhões foram gastos em operações fraudulentas nos Estados Unidos, de acordo com o U.S Department of Justice.

Os governos estudam formas de criar leis para combater esse tipo de crime, enquanto os bancos e as operadoras de cartão de crédito tomaram suas próprias iniciativas para criar normas para garantir boas práticas no uso, manuseio e armazenagem de dados de cartão de crédito: Payment Card Industry (PCI) – Data Security standard (DSS).

Fraudes de Cartão de Crédito

Fraudes eletrônicas ou fraudes de cartão de crédito são aquelas em que os dados do cartão de crédito (número, validade e código de segurança) são roubados e usados indevidamente para a realização de compras em estabelecimentos. Os estabelecimentos entregam o produto comprado e esperam receber, em alguns dias, o crédito referente àquela venda.

Ao receber a fatura do cartão de crédito, os clientes (portadores de cartão de crédito) identificam despesas que não foram feitas por eles e solicitam à administradora o cancelamento das mesmas. A administradora, por sua vez, estorna a compra do estabelecimento, que não recebe o dinheiro e já entregou o produto. O estabelecimento acaba assumindo o prejuízo da fraude.

O que é PCI-DSS?

Em setembro de 2006, algumas bandeiras de cartão de crédito, entre elas Visa, Mastercard e American Express, criaram um conselho designado a criar e recomendar as melhores práticas de segurança de dados, a serem seguidas pelos estabelecimentos comerciais que aceitam cartões de crédito como forma de pagamento, para proteger a privacidade dos consumidores portadores de cartão de crédito. Esse conselho é chamado PCI Council (www.pcisecuritystandards.org).

O PCI-DSS contempla 12 requerimentos básicos que têm o objetivo de:

1. Manter a rede de dados segura;
2. Proteger as informações de portadores de cartão de crédito;
3. Manter um programa de Gerenciamento de vulnerabilidades;

4. Implementar um forte controle de acessos;

5. Manter uma política de segurança de informações.

Não estar em conformidade com a PCI-DSS pode incorrer em multas e até em descredenciamento dos estabelecimentos comerciais em aceitar cartões de crédito.

12 Requerimentos da PCI-DSS

1. Instalar e manter um firewall para proteger dados de cartão de crédito.

2. Não utilizar senhas padrão ou outras configurações de segurança dos softwares utilizados.

3. Proteger dados de cartões de crédito armazenados.

4. Utilizar criptografia na transmissão de dados de cartões de crédito, manter um programa de Gerenciamento de Vulnerabilidades.

5. Utilizar regularmente programas anti-vírus.

6. Desenvolver e manter sistemas e aplicações seguras, implementar um forte controle de acesso.

7. Restringir acesso a dados de cartões de crédito por negócio e por pessoas que realmente precisam acessá-los.

8. Designar um único ID para cada usuário da rede e sistemas.

9. Restringir acesso físico aos dados de cartão de crédito, testar e monitorar a rede regularmente.

10. Rastrear e monitorar todos os acessos à rede e dados de cartões de crédito.

11. Testar a segurança de sistemas e processos regularmente, manter um programa de Gerenciamento de Vulnerabilidades.

12. Manter uma política que enderece informações de segurança.

Quem precisa estar em conformidade?

O PCI DSS se aplica a toda e qualquer empresa que coleta, processa, armazena ou transmite informação de cartão de crédito, estando, portanto, obrigada a se adaptar ao padrão. Em linhas gerais, esta adaptação inclui comerciantes, intermediários que processam dados de cartão de crédito e estão ligados à rede da associação de cartões, assim como provedores de serviço que hospedam sites, processam transações em ATM ou coletam e processam dados de cartão de crédito em nome de membros das redes Visa e Mastercard – gateways de pagamento.

A exceção fica com empresas que apenas emitem cartões de crédito e autorizam transações, como bancos e grandes varejistas, deixando de ser obrigados a demonstrar conformidade com o PCI DSS.

Qual o prazo e o nível de aderência atual?

O cronograma de conformidade varia de acordo com o continente e o mercado. No Brasil, as empresas físicas e virtuais que estão dentro do escopo do PCI terão até este ano (2009) para se adequarem. Entretanto, o resultado de uma pesquisa feita em 2006 no mercado norte-americano revelou que menos de 20% de todos os grandes varejistas e provedores de serviço atingiram a conformidade plena com o PCI DSS. Já em 2007, a mesma pesquisa chegou ao índice de 35% de conformidade.

Considerando a heterogeneidade dos ambientes operacionais e dos modelos de negócio das empresas envolvidas no compliance, podem surgir dificuldades em implementar alguns dos requerimentos. Nesses casos, será preciso definir e implementar controles compensatórios de forma a alcançar o nível de risco residual adequado.

Sabemos que para as empresas se adequarem às normas do PCI-DSS envolve muitos custos, portanto procure uma consultoria ou uma empresa séria para indicação de equipamentos que serão utilizados como Firewall, IPS/IDS, Anti-vírus e outros equipamentos e softwares para adequação desta norma.

Douglas Falsarella
é formado em Ciências da Computação e atualmente é sócio da DWA Consulting. Especialista em Routing & Switching bem como em projetos de Rede e Telecom, atua também como PMO em projetos de operadoras de TV e Telefonia Celular. Tem experiência em grandes empresas da área, entre elas Huawei, Alcatel-Lucent, AT&T, CTBC, Telefônica Internacional.

- **Página do autor**
- **Email**

Leia os últimos artigos publicados por Douglas Falsarella

- SDN (Software Defined Networking) e o futuro das redes
- Virtualização de servidores em redes locais
- Get IT Up Cast 6 – Raio X da internet no Brasil
- Get IT Up Cast com Marco Fabossi
- Get IT Up Cast 3 – Trabalhando fora do Brasil