Perguntas que você deve fazer aos seus fornecedores

FUNDAMENTOS DA SEGURANÇA DE DADOS PARA PEQUENOS COMERCIANTES

UM PRODUTO DA FORÇA-TAREFA DE PEQUENOS COMERCIANTES DA INDÚSTRIA DE CARTÕES DE PAGAMENTO

VERSÃO 2.0 | AGOSTO DE 2018

PCI Security Standards Council®

Introduçã

Perguntas que você deve fazer aos seus fornecedores é um suplemento do *Guia para pagamentos seguros*, que integra os Fundamentos da segurança de dados para pequenos comerciantes. Estas sugestões de perguntas a serem feitas aos seus fornecedores e prestadores de serviço foram elaboradas para ajudar você a entender como essas entidades oferecem suporte para a proteção dos dados do cartão dos clientes.

Consulte o *Guia para pagamentos seguros* e os outros Fundamentos da segurança de dados para pequenos comerciantes disponíveis em:

RECURSO	URL
Guia para Pagamentos Seguros	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Sistemas comuns de pagamento	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Glossário de termos de segurança da informação e pagamentos	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf
Ferramenta de avaliação	https://www.pcisecuritystandards.org/merchants/ Esta ferramenta é disponibilizada apenas para informação do comerciante. Uma opção para os comerciantes é usá-la como um primeiro passo para obter perspectivas sobre práticas de segurança pertinentes à forma com que aceitam pagamentos a fim de lhes propiciar respostas iniciais e lhes permitirem a visualização de seus resultados.

Fornecedores e prestadores de serviço e como eles funcionam

Devido ao fato de que, muitas vezes, pequenas empresas e comerciantes entram em contato com diversos fornecedores de pagamento ou prestadores de serviço, é importante que os comerciantes entendam o tipo de fornecedor com o qual estão trabalhando e garantam que o fornecedor tenha tomado as medidas adequadas para proteger os dados de cartões.

A tabela na página 2 descreve os tipos mais comuns de fornecedores de pagamento e prestadores de serviços e informa o que os comerciantes devem verificar em relação a cada fornecedor.

A tabela que começa na página 3 fornece aos comerciantes sugestões de perguntas para fazer aos seus fornecedores ou prestadores de serviços a fim de ajudá-los a entender a função do fornecedor ou do prestador de serviços na proteção dos dados de cartões.

Fornecedores e prestadores de serviço

A tabela abaixo descreve os tipos mais comuns de fornecedores de pagamento e prestadores de serviços, suas funções e os padrões ou programas PCI que se aplicam a essas funções. Consulte o Anexo para ver uma lista de perguntas recomendadas para cada tipo de fornecedor ou prestador de serviços.

Tipo de fornecedor/prestador de serviços	Função	Padrão ou programa do PCI	O que verificar:
Fornecedor do aplicativo de pagamento	Vender e oferecer suporte a aplicativos que armazenam, processam e/ou transmitem dados do portador do cartão.	Padrão de segurança de dados de aplicativos de pagamento (PA-DSS)	O aplicativo está na Lista do PCI PA-DSS de aplicativos de pagamento validados
Fornecedores de terminais de pagamento, fornecedores de soluções de pagamento	Vender e prestar suporte para dispositivos ou soluções (terminais de pagamento ou soluções de criptografia, por exemplo) usados para aceitar pagamentos de cartão.	Segurança de transações com PIN (PTS) Criptografia Ponto a Ponto PCI	O terminal de pagamento está na Lista de dispositivos PTS aprovados pelo PCI A solução de criptografia está na Lista de soluções PCI P2PE
Processadores de pagamento, prestadores de serviços de pagamento de e-commerce, gateways de pagamento, centrais de contato	Armazenar, processar ou transmitir dados do portador do cartão em seu nome.	Padrão de Segurança de Dados do PCI (PCI DSS)	Solicite o Atestado de Conformidade do PCI DSS do prestador de serviços e verifique se a avaliação incluiu o serviço que você está usando. Verifique se o prestador de serviços está em uma destas listas: Lista da MasterCard de prestadores de serviços em conformidade Registro global da Visa de prestadores de serviços Agentes de comerciantes registrados da Visa Europa
Provedores de hospedagem de e-commerce	Hospedar e gerenciar seu servidor ou site de e-commerce e/ou desenvolver e oferecer suporte ao seu site. Este provedor pode fornecer serviços de hospedagem apenas ou pode realizar também o processamento de pagamentos.		
Provedores de software como serviço, provedores de hospedagem baseada na nuvem	Desenvolver, hospedar e/ou gerenciar seu aplicativo da Web ou aplicativo de pagamento baseado na nuvem (por exemplo, aplicativo de emissão de tíquetes ou de reserva online).		
Provedores de serviços que podem ajudá-lo a cumprir os requisitos da PCI DSS	Gerenciar/operar sistemas ou serviços em seu nome (a exemplo de centrais de dados, provedores de centros de co-localização e serviços de tecnologia da informação, como serviços de gerenciamento de firewall, patches ou antivírus).		
Integradores/revendedores	Instalar sistemas de pagamento para comerciantes.	Integradores e revendedores qualificados (QIR)	Pergunte se o fornecedor é um integrador ou revendedor qualificado (QIR, Qualified Integrator or Reseller) da PCI. Verifique se o fornecedor está na Lista de QIRs da PCI.

Glossário

A tabela abaixo contém várias perguntas que os comerciantes devem fazer aos seus fornecedores/prestadores de serviços para determinar se os controles adequados estão em vigor para proteger os dados de cartões.

Observação: Se um fornecedor ou provedor de soluções não apresentar respostas positivas para as perguntas aplicáveis nesta tabela, considere seriamente procurar outro fornecedor ou provedor de soluções.

Pergunte:	Análise das respostas do fornecedor – Etapas úteis e informações adicionais para comerciantes
A solução ou produto do fornecedor é seguro?	
1. A solução/produto do fornecedor captura e transmite com segurança as informações dos cartões de pagamento? *Quando um produto ou serviço é listado pela PCI SSC ou pelas marcas de cartão de pagamento, isso significa que o produto/serviço foi validado de acordo com um padrão de segurança PCI. A inclusão nessas listagens é uma indicação de que o fornecedor ou prestador de serviços tomou medidas adicionais para fornecer produtos ou serviços seguros.*	**Para soluções ou produtos com terminais de pagamento ou aplicativos de pagamento:** • Verifique se o terminal de pagamento é aprovado pela PCI PTS: Lista de dispositivos aprovados pela PCI PTS E/OU • Verifique se o aplicativo de pagamento é validado pela PCI PA-DSS: Lista da PCI PA-DSS de aplicativos de pagamento validados OU • Verifique se a solução de criptografia é validada pela PCI P2PE: Lista de soluções validadas pela PCI P2PE
	Para transações de pagamento com cartão não presente (inclusive em e-commerce e encomendas por correio e por telefone): • Verifique se o prestador de serviços está em conformidade com a PCI DSS: Lista da MasterCard de prestadores de serviços em conformidade Registro global de prestadores de serviços da Visa Agentes de comerciantes registrados da Visa Europa OU • Verifique se o aplicativo de pagamento é validado pela PCI PA-DSS: Lista da PCI PA-DSS de aplicativos de pagamento validados

Perguntas

Pergunte:	Análise das respostas do fornecedor – Etapas úteis e informações adicionais para comerciantes
A solução ou produto do fornecedor é seguro?	
2. O produto/solução do fornecedor armazena as informações do cartão de pagamento em meus sistemas (que estão em meus estabelecimentos/lojas, em meu aplicativo web ou em meu site de e-commerce, por exemplo). Em caso afirmativo, como o produto/solução protege os dados?	Os produtos ou soluções que tokenizam ou criptografam informações do cartão de pagamento são uma maneira de os comerciantes protegerem os dados do cartão. Consulte o *Guia para pagamentos seguros* para obter mais informações sobre criptografia e tokenização.
3. O produto/solução do fornecedor protege os dados do cartão de pagamento durante a transmissão com criptografia forte?	A criptografia converte as informações para um formato inutilizável, exceto para os detentores de uma chave digital específica. Proteger os dados do cartão de pagamento dessa forma torna menos provável o furto desse dados e seu uso em fraudes. **Para terminais de pagamento e terminais de pagamento integrados:** • Se puder, faça sua escolha na Lista de soluções validadas pela PCI P2PE por um produto/solução em que os dados do cartão sejam encriptados. O uso de uma solução listada pela PCI P2PE significa que os dados do cartão de pagamento são protegidos assim que você os recebe e durante a viagem deles por sua rede até o processador de pagamento. **Para aplicativos de pagamento:** • Confirme com seu fornecedor, revendedor ou integrador que o aplicativo de pagamento é validado pela PCI PA-DSS. **Para sites de e-commerce hospedados, aplicativos web ou aplicativos de pagamento:** • Pergunte ao seu prestador de serviços se ele usa uma versão segura da Transport Layer Security (TLS) para proteger as transmissões de dados dos cartões de pagamento.
4. A solução ou o produto do fornecedor precisa se integrar com meus outros sistemas, como terminais de pagamento, controle de contas a receber ou outros sistemas que contenham dados do portador do cartão?	Um terminal de pagamento autônomo ou isolado é mais simples de proteger do que um sistema de pagamento mais complexo com muitos sistemas conectados. **Se a solução exigir integração com outros sistemas em seu ambiente, considere o seguinte:** • Ela simplifica seu ambiente de processamento? • Como ela vai agregar valor ao seu negócio? • Você precisa desse tipo de solução? Considere que ela aumentará o risco e a complexidade do seu negócio, aumentando o ambiente de dados do portador do cartão e tornando-o mais difícil de proteger. Talvez valha considerar outro fornecedor ou produto, a menos que seja realmente necessário ter uma solução mais sofisticada conectada com seus outros sistemas.

Perguntas

Pergunte:	Análise das respostas do fornecedor – Etapas úteis e informações adicionais para comerciantes
O fornecedor vai me ajudar a instalar ou configurar com segurança o produto ou a solução?	
5. Se o fornecedor estiver instalando um aplicativo ou sistema de pagamento em seu ambiente, pergunte: • O fornecedor é um integrador ou revendedor qualificado da PCI? • Se o fornecedor não instalar o aplicativo ou sistema de pagamento, espera-se que você o instale?	Os QIRs são integradores e revendedores especialmente treinados pelo Conselho para abordar controles críticos de segurança ao instalar sistemas de pagamento de comerciantes. Os QIRs reduzem o risco do comerciante e mitigam as causas mais comuns de violações de dados de pagamento concentrando-se nos controles críticos de segurança. Verifique se o fornecedor consta na lista: Lista de QIRs da PCI.
6. Independentemente de o fornecedor ser um QIR, se ele estiver instalando um aplicativo ou um sistema de pagamento, pergunte: • O fornecedor me oferece suporte durante a instalação e garante que ela seja feita com segurança? • O fornecedor disponibiliza um guia de implementação para me ajudar a configurar o aplicativo com segurança?	A instalação inadequada pode deixar seu sistema vulnerável a comprometimentos. O fornecedor deve instalar o aplicativo ou sistema de forma segura ou ajudar você por meio de orientações sobre a implementação. A implementação deve contemplar, no mínimo, como alterar as senhas padrão e definir senhas fortes, como gerenciar patches e atualizações e uma descrição de como o fornecedor usa o software de acesso remoto para acessar seu negócio (e qual é a sua função nesse software). Mais detalhes sobre cada uma dessas três áreas estão incluídos nas perguntas 7, 8 e 9 abaixo.

Perguntas

Pergunte:	Análise das respostas do fornecedor – Etapas úteis e informações adicionais para comerciantes
O fornecedor vai me ajudar a instalar ou configurar com segurança o produto ou a solução?	
7. O fornecedor presta suporte durante a instalação ou configuração do produto/solução para me ajudar a mudar as senhas padrão informadas pelo fornecedor? • O fornecedor me ajuda a configurar senhas fortes?	As senhas fracas e as senhas padrão informadas pelo fornecedor são uma das três principais causas de violações de dados de comerciantes (as outras duas são abordadas nas perguntas 8 e 9 abaixo). Senhas padrão informadas pelo fornecedor são aquelas que vêm com um produto ou solução, como a primeira senha de um novo sistema ou aplicativo, de um site de e-commerce hospedado pelo comerciante ou de um aplicativo de reservas de hotéis. Essas senhas padrão informadas pelo fornecedor são, muitas vezes, simples e conhecidas pelos hackers (como “admin”, “senha” ou o nome da empresa ou do produto do fornecedor). Essas senhas devem ser alteradas para uma senha forte quando o produto for instalado ou configurado pela primeira vez. Se você alterá-la para uma senha simples (como “12345”), um hacker terá facilidade para entrar em seus sistemas de pagamento. Se o fornecedor não alterar as senhas padrão ao instalar ou configurar o aplicativo ou sistema, ele deverá dar orientações sobre como alterar essas senhas e como definir senhas fortes.
O fornecedor presta suporte e faz manutenção do produto/solução com segurança?	
8. Para entender os patches (correções de segurança de software) e as atualizações para o produto/solução, pergunte ao fornecedor: • Que suporte e orientações o fornecedor disponibiliza para o meu negócio durante o processo de correção com patches/atualização? • Os patches e as atualizações são fornecidos e instalados automaticamente pelo fornecedor? • Devo obter e instalar esses patches/atualizações? • Como o fornecedor me notifica da disponibilidade de patches/atualizações ou de que eles foram aplicados automaticamente? • Em caso de sites de e-commerce hospedados, aplicativos da web ou aplicativos de pagamento, o fornecedor assume a responsabilidade de fazer as correções com patches/atualizações para a solução que eles estão fornecendo?	Aplicativos e sistemas sem patches de segurança são uma das três principais causas de violações de dados de comerciantes (as outras duas são abordadas nas perguntas 7 e 9). Os sistemas sem patches geralmente trazem vulnerabilidades que hackers conseguem usar para obter acesso aos dados do seu cartão de pagamento. O fornecedor deve prestar manutenção e dar suporte contínuos para seus aplicativos ou sistemas por meio de atualizações de software e patches de segurança (correções de segurança de software). Por exemplo, o fornecedor deve enviar os patches quando necessário, avisá-lo quando eles estiverem disponíveis e dar orientações sobre como instalá-los. É extremamente recomendável ter fornecedores que prestam suporte total para seus produtos/soluções e que assumam a responsabilidade com patches e atualizações ou auxiliem você a fazer isso a fim de garantir segurança para seu negócio, mesmo com eventuais mudanças.

Perguntas

Pergunte:	Análise das respostas do fornecedor – Etapas úteis e informações adicionais para comerciantes
O fornecedor presta suporte e faz manutenção do produto/solução com segurança?	
9. O fornecedor exige acesso remoto ao meu aplicativo ou sistema de pagamento para prestar suporte para o produto ou solução? • O fornecedor exige que o acesso remoto esteja constantemente ativo? • Que medidas o fornecedor toma para proteger o acesso remoto? • O fornecedor usa a mesma senha ou uma senha diferente para cada um de seus clientes?	O acesso remoto sempre disponível ou "always on" é uma das três principais causas de violações em comerciantes (as outras duas estão nas perguntas 7 e 8 acima). O acesso remoto é um caminho de fora da rede para a rede do comerciantes, o qual um hacker pode usar facilmente para comprometer seu sistema (ou o sistema hospedado) e obter acesso aos dados do portador do cartão. Um exemplo é o acesso remoto à rede de um comerciante, usada pelo fornecedor para prestar suporte para um terminal de pagamento ou aplicativo, ou para dar suporte a um ambiente de aplicativo web do comerciante hospedado por terceiros. Para se proteger, você deve garantir que os fornecedores ajudem você: • Limitando o acesso remoto a um breve uso periódico • Desativando o acesso remoto quando ele não estiver sendo usado • Usando autenticação multifatores (uma forma de verificar a identidade de uma pessoa que acessa um sistema por meio do uso de dois ou mais fatores, como algo que a pessoa conhece e algo que ela faz ou é) • Usando um nome de usuário e senha diferentes para cada cliente que o fornecedor acessa remotamente (para evitar o uso de um nome de usuário e senha comumente usados, causando comprometimento a todos os seus clientes)
O fornecedor está em conformidade com a PCI DSS no que se refere ao serviço que está me oferecendo?	
10. Essa solução ou produto roda em sistemas de propriedade e manutenção (hospedados) do fornecedor? Isso significa que seu fornecedor é um prestador de serviços. **Pergunte:** • O ambiente do prestador de serviços é conforme ao PCI DSS? • A avaliação da PCI DSS do prestador de serviços abrange os serviços específicos que ele está me oferecendo?	Isso é considerado um "serviço gerenciado". Solicite o Atestado de Conformidade do PCI DSS do prestador de serviços e verifique se a avaliação incluiu o serviço que você está usando. Verifique se o prestador de serviços está em uma destas listas: Lista da MasterCard de prestadores de serviços em conformidade Registro global de prestadores de serviços da Visa Agentes de comerciantes registrados da Visa Europa
11. O acordo do fornecedor com você inclui cláusulas que afirmam que o fornecedor manterá a conformidade com a PCI DSS para os serviços (ou terá validação da PCI DSS)?	Fornecedores que oferecem serviços (também chamados de prestadores de serviços) que estão ou ficarão em conformidade com a PCI DSS devem estar dispostos a concordar com que essa situação seja incluída em um contrato por escrito. Verifique se o prestador de serviços está em uma das listas contidas na pergunta 10 acima.

Perguntas

Pergunte:	Análise das respostas do fornecedor – Etapas úteis e informações adicionais para comerciantes
O fornecedor prestará suporte se houver violação dos dados do titular do cartão?	
12. Se houver violação de dados e o produto/solução do fornecedor estiver envolvida, pergunte: • Que monitoramento para violações de dados e atividades suspeitas você fornece? • Como e quando você me notificará se houver uma violação? • Se eu for processado/multado, você oferece suporte e proteção?	O fornecedor ou prestador de serviços deve fornecer suporte no caso de uma violação de dados do portador do cartão. O fornecedor ou prestador de serviços deve concordar em cooperar com um investigador forense se houver dúvidas sobre o serviço ou produto/solução gerenciada que ele oferece. O fornecedor/prestador de serviços deve concordar em ajudar você em caso de multas por violação e se for determinado que o produto/solução do fornecedor foi a causa.
13. O fornecedor ou prestador de serviços possui seguro para cobrir as violações de dados relacionadas ao seu produto ou solução?	Ter um seguro demonstra que o fornecedor ou prestador de serviços pensou em sua responsabilidade em relação a violações de dados de portadores de cartões. Se ele tiver seguro, pergunte sobre a amplitude da cobertura e se sua implementação será coberta.
14. O fornecedor ou prestador de serviços auxiliará na notificação de meus clientes caso ocorra uma violação de dados quando o produto/solução do fornecedor for a causa?	Os fornecedores ou prestadores de serviços devem estar dispostos a ajudar os comerciantes com notificação sobre violação quando seu sistema de pagamento for a causa da violação.
15. Se a resposta à pergunta 14 for afirmativa, até que ponto o fornecedor ajuda com a notificação? O fornecedor: • Cobre o custo? • Envia as notificações? • Oferece monitoramento de crédito para os clientes afetados?	Se o fornecedor não ajudar com a notificação, você deverá desenvolver um plano para notificar seus clientes caso haja violação dos dados de titulares de cartões.

Anexo

Quais perguntas se aplicam a quais fornecedores/ prestadores de soluções?

Tipo de fornecedor/prestador de serviços	Perguntas pertinentes
Fornecedor do aplicativo de pagamento	1-15
Fornecedores de terminais de pagamento, fornecedores de soluções de pagamento	1-15
Processadores de pagamento, prestadores de serviços de pagamento de e-commerce, gateways de pagamento, centrais de contato	1-15
Provedores de hospedagem de e-commerce	1-15
Provedores de software como serviço, provedores de hospedagem baseada na nuvem	1-4 e 1-15
Prestadores de serviços que podem ajudar você a cumprir os requisitos da PCI DSS	1-15
Integradores/revendedores	5-9