Como o PCI DSS pode ajudar trabalhadores remotos

O PCI SSC envia orientações para proteger as informações de pagamento e sobre como trabalhar com segurança ao acessar e trabalhar remotamente. **Como manter a segurança no trabalho remoto?**

Tudo se resume a pessoas, processos e tecnologia. Os funcionários são a primeira linha de defesa, e as equipes que trabalham remotamente pela primeira vez podem não estar familiarizadas com as políticas e os processos da organização que se aplicam a ambientes de trabalho remotos. Todos os membros das equipes devem receber treinamento de conscientização de segurança, com ênfase na importância da segurança de dados, e devem conhecer as políticas e os processos de segurança da organização que se aplicam ao trabalho remoto. Por exemplo, as políticas e os procedimentos devem proibir claramente qualquer cópia, movimentação, compartilhamento ou armazenamento não autorizado de dados de cartões de pagamento em ambientes remotos. As equipes remotas também precisam estar cientes de seu ambiente físico, com cuidado para evitar que informações confidenciais sejam consultadas por pessoas não autorizadas.

Os processos de segurança da organização devem ser mantidos atualizados e prontos para qualquer eventualidade causada por ameaças provenientes de ambientes remotos. O uso de tecnologias que garantam que as informações de pagamento permaneçam protegidas e que permitam que as equipes remotas realizem o trabalho com segurança também é uma consideração vital no apoio dos ambientes de trabalho remotos.

Como o Padrão de Segurança de Dados do PCI (PCI DSS) apoia o trabalho remoto seguro?

O PCI DSS apresenta diversos requisitos de segurança, que devem ser implementados para proteger trabalhadores remotos e seus ambientes. Alguns exemplos:

- Utilize autenticação multifator para todo o acesso remoto à rede proveniente de fora da rede da empresa.
- Se forem utilizadas senhas, aplique uma política de senhas fortes e não permita o uso de senhas compartilhadas. Instrua as equipes sobre a importância de proteger as senhas e outras credenciais de autenticação contra o acesso não autorizado.
- Assegure que todos os sistemas usados pelas equipes que trabalham remotamente sejam atualizados, possuam proteção anti-malware e recursos de firewall para proteção contra ameaças baseadas na Internet.

- Desinstale ou desative os aplicativos e software que não forem necessários, para reduzir a superfície de ataque de computadores e laptops.
- Implemente controles de acesso para garantir que somente os indivíduos cujo trabalho exigir o acesso ao ambiente de dados do titular do cartão (CDE) ou aos dados do titular do cartão tenham acesso a esses recursos.
- Utilize somente comunicações seguras e criptografadas, como uma VPN configurada corretamente, para proteger todas as transmissões com origem ou destino no dispositivo remoto que contiver informações confidenciais, como dados de titulares de cartões.
- Desconecte automaticamente as sessões de acesso remoto após um período de inatividade, para evitar que conexões ociosas e abertas sejam usadas para acesso não autorizado.
- Limite o acesso aos componentes de sistema e aos dados de titulares de cartão apenas àqueles indivíduos cujo trabalho exige tal acesso.
- Assegure-se de que os planos de resposta a incidentes estejam atualizados e incluam detalhes de contato precisos de funcionários essenciais. Os procedimentos para detectar e responder a uma possível violação de dados podem ser diferentes em incidentes provenientes de ambientes de trabalho remotos.

Há considerações diferentes entre o processo de segurança de dados de pagamento e o de ambientes locais e remotos?

Os métodos para manter e garantir a eficácia de processos e controles seguros podem precisar ser aplicados de forma diferente entre ambientes locais e remotos. Por exemplo, a verificação da identificação de um usuário que chama a TI para receber suporte pode envolver etapas diferentes quando o usuário e o departamento de TI estão no mesmo local.

Todas as equipes devem ser treinadas para estarem cientes de possíveis chamadas de phishing. As equipes de TI devem estar preparadas para identificar chamadas fraudulentas de pessoas que afirmam ser usuários remotos, e deve haver um processo para que as equipes confirmem a identidade daqueles que acionarem o suporte de TI remotamente. Da mesma forma, as equipes remotas devem saber como confirmar que uma pessoa que telefona alegando ser de TI corporativa é legítima antes de fornecer qualquer informação.

Todas as organizações devem avaliar os riscos adicionais associados ao processamento de dados de pagamento em locais não seguros e implementar controles corretamente. Todo o pessoal deve estar plenamente ciente dos riscos relacionados ao trabalho remoto e do que é necessário para manter a segurança constante de sistemas, processos e equipamentos que apoiam o acesso e o processamento seguros dos dados de cartões de pagamento.

Onde encontro mais informações?

Para mais informações sobre como proteger o acesso remoto, consulte os recursos do PCI SSC:

- Infográfico: **Princípios básicos de segurança de dados de pagamento: acesso remoto seguro**
- Página web: **Recursos de segurança de pagamentos para comerciantes**
- Blog: **Como proteger pagamentos no trabalho remoto**

Proteção de pagamentos no trabalho remoto