SEGURANÇA ESSENCIAL DOS DADOS DE PAGAMENTO

Acesso remoto seguro

QUAL É O RISCO?

#1

Ponto de entrada para ataques contra comerciantes de lojas físicas é o acesso remoto inseguro

(Práticas recomendadas da tecnologia de acesso remoto)

O acesso remoto inseguro é uma das principais causas de violações de dados nas empresas.

Os fornecedores de ponto de venda (PDV) geralmente oferecem suporte ou solucionam problemas nos sistemas de pagamento do comerciante a partir de seus escritórios e não no local das empresas. Eles atuam por meio da Internet com o que é conhecido como produtos de software de "acesso remoto". Muitos desses produtos estão sempre ativos ou sempre disponíveis – o que significa que o fornecedor pode acessar seus sistemas de forma remota em tempo integral.

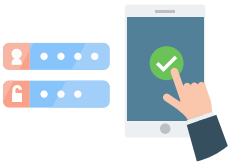
Muitos desses fornecedores utilizam senhas comumente conhecidas no acesso remoto, tornando muito fácil para os hackers acessarem seus sistemas também. Eles varrem a Internet em busca de empresas com sistemas de acesso remoto vulneráveis e, uma vez dentro, usam malware para roubar dados valiosos de cartões de pagamento.

PRÁTICAS RECOMENDADAS PARA O ACESSO REMOTO

Para minimizar o risco de violação, é importante que você participe do gerenciamento de como e quando seus fornecedores podem acessar seus sistemas. Permita o acesso remoto somente quando necessário!

Limite o uso do acesso remoto

Pergunte a seus fornecedores como habilitar o acesso remoto quando solicitarem especificamente e como desativá-lo quando não for necessário.



Solicite o uso de autenticação multifator

Se você precisar autorizar o acesso remoto, peça aos fornecedores que usem a autenticação multifator para dar suporte à sua empresa.

Solicite credenciais exclusivas

Se você precisar autorizar acesso remoto, verifique se os seus fornecedores utilizam credenciais de acesso remoto exclusivas para sua empresa e se não são as mesmas utilizadas com outros clientes.

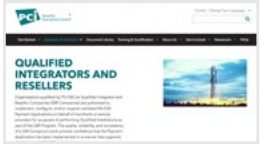
A autenticação multifator protege o acesso remoto à sua empresa, solicitando um nome de usuário e uma senha, além de outro fator (como um cartão inteligente ou dongle). Um dongle é um dispositivo útil que se conecta a um computador e permite o acesso a recursos sem fio, software, etc.

RECURSOS

Acesse ***pcissc.org/Merchants*** para mais recursos

O recurso do PCI SSC perguntas a serem feitas a seus fornecedores pode ajudar as empresas a receberem as informações de que você precisa de seus fornecedores de terceiros.

O guia para pagamentos seguros apresenta às empresas a segurança básica para se protegerem contra roubo de dados de pagamento.



A lista de integradores e revendedores qualificados (QIR) é um recurso que as empresas podem usar para encontrar instaladores de sistemas de pagamento, treinados pelo PCI Security Standards Council no acesso remoto seguro, e outros elementos essenciais de segurança de dados de pagamento.

Assista a este breve vídeo de animação para aprender como as empresas podem minimizar as chances de violação, autorizando o acesso remoto quando necessário e utilizando autenticação multifator.

PCI Security Standards Council