Patches

QUAL É O RISCO?

80%

dos ataques de hackers podem ser evitados fortalecendo as senhas e instalando correções de software

(Relatório de Investigação de Violação de Dados Verizon 2017)

Software sem correções é uma das principais causas de violações de dados nas empresas.

Geralmente, o software tem falhas ou erros cometidos pelos programadores que escreveram o código. Os fornecedores emitem atualizações regularmente, conhecidas como correções ou "patches", para solucionar essas vulnerabilidades de software. Quando as empresas não aplicam as correções de software dos fornecedores, os hackers exploram essas vulnerabilidades para invadir computadores e sistemas e roubar dados de pagamento.

PRÁTICAS RECOMENDADAS PARA CORREÇÕES

A instalação oportuna de correções de segurança é muito importante para minimizar o risco de violação. Para aplicar correções de forma rápida, é importante que você saiba como seu software está sendo atualizado regularmente com correções e quem é o responsável (pode ser você!).

Identifique quais fornecedores enviam correções

O recurso Perguntas a fazer aos seus fornecedores pode ajudar as empresas a identificarem quais fornecedores enviam correções. São os fornecedores de terminais de pagamento, aplicativos de pagamento, outros sistemas de pagamento (caixas registadoras, PCs, etc.), sistemas operacionais (Android, Windows, iOS, etc.), aplicações (incluindo seu navegador da web) e software de negócios.

Converse com seus fornecedores sobre as correções

É importante que seus fornecedores atualizem seus terminais de pagamento, sistemas operacionais, etc para que possam aplicar as correções de segurança mais recentes. Pergunte a eles como as correções são adicionadas (algumas são instaladas automaticamente quando ficam disponíveis) e quem é o responsável. Descubra como avisam sobre novas correções de segurança e não deixe de receber e ler esses avisos.

Instalação de correções

Siga as instruções dos fornecedores e instale as correções o quanto antes.

Não ignore o e-commerce

As empresas de e-commerce devem procurar as correções junto ao provedor de serviços de pagamento. Pergunte ao seu provedor de hospedagem de e-commerce se eles têm correções para seu sistema (e com que frequência as oferecem). Certifique-se de que eles atualizam o sistema operacional, a plataforma de e-commerce e/ou o aplicativo da web para que possa suportar os correções mais recentes.

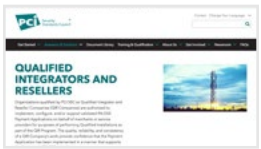
RECURSOS

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

O recurso Perguntas a fazer aos seus fornecedores pode ajudar as empresas a identificar quais fornecedores enviam correções.

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

Assista a esta breve animação para saber como as empresas podem minimizar as chances de serem violadas, instalando correções de software rapidamente.



Ferramentas de verificação de vulnerabilidades fornecidas pelos fornecedores de verificação aprovados do PCI podem também ajudar as empresas a pesquisarem automaticamente as suas redes, para localizar vulnerabilidades e informar quando as correções precisam ser aplicadas.

A lista de revendedores e integradores qualificados do PCI (QIR) é um recurso que as empresas podem utilizar para encontrar instaladores de sistemas de pagamento, treinados pelo PCI Security Standards Council sobre correções e outros elementos essenciais de segurança de dados de pagamento.

PCI Security Standards Council