パッチ

リスクは何か？

80%

強化することで パスワードとソフト ウェアパッチのイン ストール

(Verizon Data Breach Investigations Report 2017)

パッチを適用していないソフトウェアが、企業にとってデータ漏洩の主な原因のひとつとなっています。

多くの場合、ソフトウェアにはプログラマがコードを作成したときにできた欠陥や不具合があります。ベンダは、これらのソフトウェアの脆弱性を修正する、パッチと呼ばれるアップデートを定期的に発行しています。企業がベンダのソフトウェアパッチを適用しないと、ハッカーは脆弱性を悪用してコンピュータやシステムに侵入し、ペイメントデータを盗み出します。

パッチ適用のベストプラクティス

侵害のリスクを最小限に抑えるには、セキュリティパッチを適切なタイミングでインストールすることが不可欠です。パッチをすばやく適用するには、ソフトウェアがパッチによって定期的に更新される方法と、更新の担当者を把握しておくことが重要です（これはあなたかもしれません）。

どのベンダがパッチを送付するのか特定する

ベンダに訊くべき質問リソースで、企業はどのベンダがパッチを送付するのか特定できます。このリソースには、ペイメント端末のベンダ、ペイメントアプリケーション、その他のペイメントシステム（現金箱、レジ、PC など）、オペレーティングシステム（Android、Windows、iOS など）、アプリケーションソフトウェア（利用中のウェブブラウザを含む）、ビジネスソフトウェアが含まれます。

パッチについてベンダと話し合う

最新のセキュリティパッチをサポートできるように、ベンダがペイメント端末、オペレーティングシステムなどをアップデートしていることを確認してください。パッチはどのように追加されるのか（利用可能になると自動的にインストールされる場合があります）、担当者は誰なのかを確認します。新しいセキュリティパッチが通知される方法を確認し、確実に通知を受け取って読むようにします。

パッチのインストール

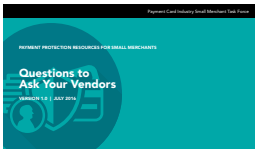
ベンダの指示に従い、できるだけ早くパッチをインストールします。

電子商取引を無視しない

電子商取引の事業者は、ペイメントサービスプロバイダのパッチに注意する必要があります。
システムにパッチを適用するかどうか（およびその頻度）については、電子商取引のホスティングプロバイダにお問い合わせください。最新のパッチをサポートできるように、オペレーティングシステム、電子商取引プラットフォーム、Web アプリケーションがアップデートされていることを確認してください。

リソース

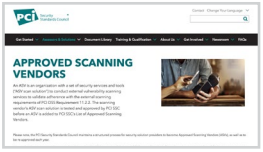
リソースについては、pcissc.org/Merchants



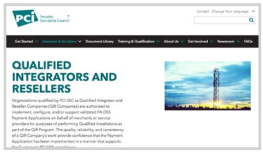
ベンダに訊くべき質問リソースで、企業はどのベンダがパッチを送付するのか特定できます。

安全な決済のためのガイドは、ペイメントデータを盗難から守るためのセキュリティの基本を企業に提供します。

このビデオでは、ソフトウェアパッチをすばやくインストールすることで、ビジネスが侵害される可能性を最小限に抑える方法をご紹介します。



PCI 認定スキャニングベンダが提供する脆弱性スキャンツールでは、ネットワークを自動的に検索して脆弱性を検出し、パッチを適用する必要がある場合に報告することもできます。



PCI 認定インテグレータ/リセラ（QIR）リストのリソースを使用して、企業はパッチの適用、およびその他のペイメントデータセキュリティの必須事項について、PCI セキュリティ基準審議会によるトレーニングを受けたペイメントシステムのインストーラを見つけることができます。

© 2020 PCI Security Standards Council LLC.
www.pcisecuritystandards.org

PCI Security Standards Council