セキュアなリモートアクセス

リスクは何か？

#1

実店舗の加盟店への攻撃の入口は、安全でないリモートアクセス

（リモートアクセステクノロジのベストプラクティス）

安全でないリモートアクセスは、企業にとってデータ侵害の主な原因のひとつとなっています。

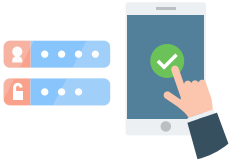
販売時点情報管理（POS）ベンダはしばしば、加盟店のペイメントシステムをビジネス拠点からではなく、オフィスからサポートまたはトラブルシューティングします。これは、インターネットと「リモートアクセス」ソフトウェア製品を使用して行います。こういった製品の大半は、常時稼働しているか、いつでも利用可能な状態であり、ベンダはいつでもリモートでシステムにアクセスすることができます。ベンダの多くは、リモートアクセス時に一般的なパスワードを使用しているため、ハッカーも簡単にシステムにアクセスできてしまいます。ハッカーは、インターネット上で脆弱なリモートアクセスシステムを持つ企業をスキャンして内部に侵入し、悪意のあるマルウェアを使用して重要なペイメントカードデータを盗み出します。

リモートアクセスのベストプラクティス

漏洩のリスクを最小限に抑えるには、ベンダがシステムにアクセスできる方法とタイミングの管理に関与する必要があります。必要な場合のみ、リモートアクセスを許可するようにしてください。

リモートアクセスの使用を制限する

特定の要求時にリモートアクセスを有効にする方法と、不要なときに無効にする方法を、ベンダに問い合わせてください。



多要素認証の使用を依頼する

リモートアクセスを許可する必要がある場合は、ベンダに多要素認証を使用して業務をサポートするよう依頼してください。

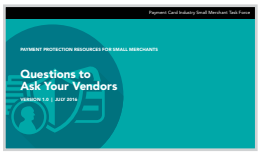
一意の認証情報を依頼する

リモートアクセスを許可する必要がある場合は、ベンダにリモートアクセスの認証情報を使用するよう依頼してください。これらの認証情報は、自分の業務に固有であり、他の顧客に使用されたものとは異なるものでなければなりません。

多要素認証では、ユーザー名とパスワードの他に、スマートカードやドングルなどの要素を要求して、ビジネスへのリモートアクセスを保護します。ドングルは、コンピュータに接続することで、ワイヤレス機能やソフトウェア機能の利用を可能にする便利なデバイスです。

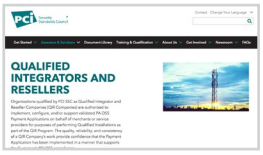
リソース

リソースについては、pcissc.org/Merchants



PCI SSC ベンダに訊くべき質問リソースで、企業は必要とする情報をサードパーティベンダから入手できます。

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。



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、企業は安全なリモートアクセス、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セキュリティスタンダードカウンシル（PCISSC）によるトレーニングを受けたシステムのインストーラを見つけることができます。

このビデオでは、必要な場合のみリモートアクセスを許可し、多要素認証を使用することで、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 Security Standards Council