リモート業務におけるペイメントの保護

PCISSC はリモート業務においてペイメントの安全を維持する方法についてのガイダンスをご紹介します。

PCI SSC はコロナウイルス(COVID-19)問題による状況の変化が起きる中、ペイメント業界に対し必要なガイダンスを提示することで貢献していいます。現在の状況ではより国際化した組織に対しリモートワークモデルへのシフが迫られています。組織のこのような動きによりペイメントカードデータを保護するためにセキュリティ業務の維持が重要です。以下はリモートワークのベストプラクティスについて PCI SSC インフォメーションサプリメントからの抜粋です“Protecting Telephone-Based Payment Card Data”.

注意: 下記を含むインフォメーションサプリメント とその抜粋は いかなる PCI SSC 基準に置き換わるものではありません

人材教育

組織内でリスクを緩和するための最善の方法のひとつはセキュリティ文化を創生・維持することです。リモートワークのためのコントロールの例としては以下のものがあります:

- セキュリティ啓蒙プログラムの実施（PCI DSS 要件 12.6），全てのスタッフが適正にトレーニングされビジネスセキュリティの方針や手続きについて知識を得ることを確実にするために新規採用時および少なくとも年 1 回実施する。これには全て

のインハウスおよび在宅•リモートワークのエージェントについてセキュリティポリシーと手続きがバイパスされたり忘れ去られたりしないように少なくとも年１回のレビューを含む。 ベストプラクティスとして個人の毎日のサイン-インの手続きの一部にセキュリティポリシーの承認を求めることも検討する

- 在宅勤務者には特別な注意が必要である。実際、コントロールの例のいくつかは実施が困難である。組織は安全でない地域ではアカウントデータの処理に関連した追加リスクを評価しそれに応じて実行すべきである。 全てのスタッフはリモートワークに関係するリスクと電話ベースでの決済につきサポートシステム、処理、装置など運用されているセキュリティを維持するために求められていることについて完全に認識すべきである

- 在宅勤務地環境に所在するシステムとデータの安全を強要することは難しい可能性がある。少なくとも在宅勤務者はアカウントデータを処理するために使うシステムと当事者がアクセスするいかなるアカウントデータが安全に維持され承認されない人物のアクセスができないことを確実にすることが求められる

処理

オフィスワーカーと在宅勤務者が電話でカード決済を処理する物理環境では効果的なモニタリングとアクセスコントロールが行われるべきです。 求められるコントロールの例としては下記のものを含みます:

- 在宅でのリモートワーカーはアカウントデータを処理するシステムもしくは環境に接続する場合は多要素認証を採用する

- ネットワーク通信ハードウェアだけでなくペメントカードデータを含むメディア、例えば電話やスクリーンの記録などへのアクセスを制限する

- もしアカウントデータが紙に記載またはプリントされていた場合、それが安全に保管されており不必要になった時点で断裁廃棄されることを確実にする。 もし、電話環境の一部がサードパーティに外注委託されている場合、そのサービスプロバイダーと委託者は各システム、処理、スタッフそして文書など安全性について責任を明確化すべきである

テクノロジー

あなたのシステム内でペイメントデータの潜在的リスクを最小化する場合、スコープやバリデーションを簡素化し犯罪者の標的になる機会を削減することが重要です。リモートワーカーへの推奨事項には下記が含まれます:

- 全てのスタッフに対し会社が承認したハードウェアのみの使用を求める、例えばモバイル、ハンドセット、ラップトップ、デスクトップとシステムこれは事業者が電話ベースでのペイメントデータの処理サポートするシステムとテクノロジーをコントロールし維持できるので特にリモート在宅勤務に関係する

- リモートによる在宅勤務環境においてすべてのデスクトップ端末は下記のようであることを確実にする:
    - 個別ファイアウォールがインストールされ運用されている
    - コーポレートウィルス防御ソフトウェアと定義ファイルが最新の状態になっている
    - 最新の承認されたセキュリティパッチがインストールされている
    - セキュリティコントロールが不能化されないように設定されている

- 在宅リモートワーカーが事業者のネットワークの延長をサポートする場合、彼らの環境(例えば、ネットワークと他のテクノロジー)が PCI DSS 要件に則して安全であることを確認する。いかなる実行もアクワイアラまたは国際ブランドとの合意のうえで行われるべきである

上記は多くは PCI SSC インフォメーションサプリメント Protecting Telephone-Based Payment Card Data からの抜粋です。このサプリメントは Council Special Interest Group (SIG) の活動成果として策定されました。SIG は PCI 基準に関係する困難に対し議論をする活動です。詳細は、Special Interest Group ページをご覧ください。.

2020 年 3 月