COVID-19 影響下でリモート評価(アセスメント)を行う場合の追加的な考慮

PCI SSC は COVID-19 に関係して現在の特殊な環境下において、事業者が世界的なパンデミックに関連する新たな、また未知の課題に対処しながらどのようにペイメントセキュリティと評価(アセスメント)活動を支援できるかを問われていることを認識しています。

PCI SSC は事業者が置かれている環境下でのセキュリティの維持とペイメントカードデータ保護を支援することに常に集中しています。私たちはビジネスが前進し続けることの重要性を理解し現在の特異な環境下でもステークホルダーのためにこの目的を支援するために専念しています。

PCI SSC はコンプライアンスプログラムを運営管理しておりませんのでコンプライアンス上の影響についてコメントすることはできませんが、この期間中において事業者と評価者がアセスメントプロセスを支援するための有用なガイダンスを提供するために取り組んでおります。現在敷かれている国際的な旅行制限や自粛により起きている影響のひとつに、評価者が事業者の所在地にて PCI のオンサイト評価を完了することができなくなっていることがあります。このブログは、以前事業者と評価者に投稿されているブログ(Remote Assessments and the Coronavirus)に特異な環境下で対応につき追加的な方向性を提示しています。

> ***注意:*** *国や地域により影響が異なり、異なるタイプの制限が設定されることがありますが、PCI SSC が全ての地域に跨るリモート評価の実行可能性について普遍的な立場を示すことは不可能です。既存のプログラム要件に準じてどのレベルの評価が可能か、環境に応じた評価の可用性は各地域や国の中で置かれた状況を元に個別に判断される必要があるでしょう。*

リモートで実行可能な評価(アセスメント)項目を特定.

オンサイト評価は常に適用される PCI SSC プログラムテスト要件、手続きそして評価合意契約に沿って可能な領域につき実行されるべきです。オンサイト評価が実行され、または実行可能であれば評価者と事業者は通常の評価を完了させ、バリデーションドキュメントを提出するべきです。

オンサイト評価が一時的に不可能な場合、評価者と事業者はどのテスト手続きがリモートで実行可能か特定するために連携するべきです。一般にリモート評価により適合するテスト手続きには次のような項目が含まれますが、個別の状況に依存します:

- ドキュメントのレビュー: 例えば、方針や手続き関連のドキュメント
- 生成されたエビデンスのレビュー: 例えば、スタッフのセキュリティ担当責任と承認の記録
- インタビュー: 例えば、スタッフが方針と手続きを理解していること、また個人のセキュリティ担当責任と承認の記録に従って処理を述べられることを確認

リモートでのドキュメントまたエビデンスのレビューに際し考慮されるべき事項にはマテリアルの共有やアクセスにはセキュアな手法が採用されること、またセキュアなシステム・環境内でのみレビューされることを含みます。評価者はさらに提供された情報の完全性、そして目視した事象がオンサイトのロケーションで行われていたことを確認する必要があるでしょう。

リモートインタビューについて考慮されるべき事項には効果的なコミュニケーション手法が採用され参加者にとり便利な時間帯に行われることを含みます。コミュニケーションの効果を最大にする技術にはインタビュー時間中はすべての参加者が可視化されるようにビデオの活用なども含まれます。

その他のテストがリモートで可能かどうかはテスト要件の詳細と評価される環境に依存するでしょう。

いつの場合でも評価機関は適用されるプログラム要件に則して評価期間中に収集された情報の機密性を維持する方針と手続きを保持することが求められます。これらの要件の詳細は適合する PCI SSC 評価者プログラムドキュメントに定義されています。

リモート評価は必ずしも可能ではない

現在の状況と旅行制限のために多くの事業者は要員を一時的に削減したり社員や訪問者の施設を一時的に閉鎖したりしなければならなくなっています。事業者はリモートによる評価行為をすすめるための準備に対応可能な十分なスタッフを確保できない可能性があります。

さらに、リモートでの評価を支援するスタッフが所在する場所ではリモートで対応可能な評価領域を限定してセキュリティと業務運用を実施している可能性があります。

リモート評価が可能な範囲を検討する場合、以下の方針が固持されるべきです。

1. リモート評価により評価される環境のセキュリティを弱体化させたりネガティブな影響を及ぼしてはならない。これにはリモート評価を容易化するために事業者にセキュリティコントロールを不可能化したり回避を求めたりする行為を含む。
2. リモート評価ではその基準への環境を評価するために PCI 基準のセキュリティ要件の違反を求めてはならない。例えば、もし PCI 基準が指定された領域内で個人のカメラ付き電話を禁止されている場合、そのようなデバイスはそのような指定領域内でリモート評価を実行する目的のために使われてはならない。
3. リモート評価は事業者の業務に支障を招くような追加的なリスクを避けることを意図するように設計され実施されなければならない。

4. リモート評価ではオンサイト評価と同レベルの厳格、完全性を維持し、評価されたコントロールが適格に実施されているかどうかについて同レベルの確実性を提示しなければならない。

テスト作業は物理的なセキュリティコントロールと実行されている処理の観察を求められている評価者にとり、一般的にリモート評価で最も困難な部分です。評価者がオンサイトで本来の活動を通じて処理を観察するのは、セキュリティ処理が正しく実施されているかどうかについて正確なドキュメントを作成し、環境についての真実の写真を取得するための唯一の方法です。

評価者と事業者双方がリモート評価の性質と実施可能性について、適用可能なテスト要件の意図と原則の確実性を維持しながら合意のうえ意見を共有すべきです。

事業者はコンプライアンスプログラムの運営サイド、すなわち国際ブランドやアクワイアラ、に対しリモートアゼスメントに関連するコンプライアンス上の影響について判断するために連絡を取るべきです。評価の実行が困難な場合、事業者は部分準拠や未完了評価、評価の遅れなどへの対応につきアクワイアラもしくは国際ブランドに相談すべきです。コンプライアンス上の例外措置や期限の延期措置など国際ブランドおよびアクワイアラにより検討されています。

リモート評価の文書化

リモートテストの結果を文書化する場合、評価者は要件およびテスト手続きがリモートで実施されたことを適合するレポート(ROC や ROV)内で明確に特定すべきです。全ての評価において評価者のアプローチが弁護されるようにしなければなりません。評価者はテストの結果と指摘事項を裏付ける作業シートの中にテストのエビデンスを維持することが求められます。

要件がオンサイトもしくはリモートで評価不可能な場合、評価者は当該要件が“not tested”であるとしてレポートで記載すべきです。事業者のコンプライアンスに影響を及ぼすバリデートされない要件に対する質問は事業者のアクワイアラや国際ブランドと協議すべきです。

PCI SSC ウェブサイト上にリストに影響を及ぼす評価への考慮

評価が定義されたテスト手続きに則して実行可能な場合、それらは通常どおりに完了され PCI SSC に提出されるべきです。PCI SSC はいかなる場合でも“not tested” とマークされた要件を含む提出物は受理しないことを注意してください。

適用される PCI 基準およびプログラムに則して評価が完了できない場合の支援について、PCI SSC は現在追加的な柔軟性を提供するプログラム指定の選択肢について検討中です。これらには PCI SSC ウェブサイト上にリストされたソリューションの再評価期限の延長や猶予期間の引き上げなどを含みます。これらのオプションが可能になった時点で各プログラムのリストページ上に詳細の情報がアップロードされます。

セキュリティの維持は極めて重要

事業者がこの期間にセキュリティコントロールの有効性を維持、監視続けることは非常に重要です。これには全ての求められるセキュリティコントロールが常に適正に配置され効果的に稼働していることを確実にすることを含みます。 Attackers thrive in times of disruption に紹介された手口、そしてこのような危機的な期間において犯罪行為が増加しています。

PCI SSC はペイメントカードデータの流出から事業者自身とその顧客を保護するために貢献いたします。最新のガイダンスについては PCI SSC ウェブサイト COVID-19 page をご確認ください。

2020 年 4 月