ファクト シート

サイバー攻撃は現実のものです お客様の備えは十分ですか？

エグゼクティブ 漏洩シミュレーション

verizon

サイバー攻撃が起こること、そしてそれが頻繁に発生して重要なデータが危険に晒されていること、残念ながらこれが現実です。事前にインシデントがいつ発生するのか、インシデントから身を守る準備ができているのか知ることで、その後のすべてが違ってきます。

インシデントにビジネスを止められてしまう前にそうした危険を防止することはできますか？お客様のインシデント対応計画を評価する定期的なテストこそが、それを知る唯一の方法です。危険を想定するだけでは安全とは言えません。お客様はその計画が有効に働いているかどうか知る必要があります。

本当に準備できているか知る「真」の方法

エグゼクティブ　漏洩シミュレーションサービスは、現在のインシデント対応計画を評価して、セキュリティ機能の向上とそのプロセスをサポートします。Verizon　RISK[1]チームのコンサルタントは、あなたの計画と現実とのギャップを特定するために脅威の模擬訓練を行います。

エグゼクティブ 漏洩シミュレーションを使って模擬訓練を実施することで、インシデント対応計画のどこに現実とのギャップがあり、どこが優れているのか確認してください。

200,000以上
のインシデント

私たちのRISKチームは、10年以上にわたってセキュリティインシデントデータを収集し、調査してきました。

私たちは、データ漏洩・侵害を含むさまざまなITセキュリティインシデントへの対応状況についてテストします。

- 封じ込め、消去、リカバリ対策における計画内のギャップを特定します
- ステークホルダーの役割を定義し、コミュニケーションとエスカレーションのプロセスを確立します
- 必要な調整作業を特定し、ステークホルダーが責任の所在を明確にできるようにしてコラボレーションを促進します
- 役員の意識を高めてセキュリティアジェンダを促進します

徹底的なテストで安心を確保

脅威の状況が日々刻々変わる中で、インシデント対応計画の定期的なテストは、将来の脅威に備える最良の方法です。エグゼクティブ漏洩シミュレーションでは、現実世界の漏洩/侵害シミュレーションに対して防衛計画をテストし、実際の攻撃に備え準備状況を確認できます。

私たちのRISKチームの知識とスキルは、世界中の組織を守るために使われます。このために私たちは以下のことに専念します:

- 変化の激しいリスク環境の調査（Researching）
- セキュリティインシデントの調査（Investigating）と対応
- 信頼できるデータと分析に基づくソリューション（Solution）の開発
- Verizon、クライアント、セキュリティコミュニティそれぞれの知識（Knowledge）の育成

より詳しい情報は

攻撃を受けることを想定したときのセキュリティ計画の有効性を確認してください。アカウントマネージャーにご連絡いただくか、

http://verizonenterprise.com/solutions/security

にアクセスしてください。

1. Research（調査・研究）, Investigations（調査）, Solutions（ソリューション）, Knowledge（知識）

FS16080 12/15