Secureworks

ホワイトペーパー

インシデント対応の担当者によく寄せられる5つの質問

セキュリティリーダーや現場の方々から、セキュアワークスの専門家によく寄せられる質問をまとめました。

セキュアワークスに寄せられる質問を回答と共有することで、他の企業・組織のご担当者がどんな疑問を持っているのか、ぜひご参考にしていただけますと幸いです。

1.組織のサイバーセキュリティインシデント対応計画（CIRP）によく見られる問題点は何ですか？

以下のケースの場合、お客様のCIRPに問題があるかもしれません。

- CIRTがテストされていない。
- 主題が抜けている、または詳細が不十分である。
  - 役割と責任があいまいである。
  - 事業継続計画、災害復旧計画、危機管理計画などの他の計画やプロセスと適切に統合されていない。
  - サードベンダーがどのように活用されるのか、明確になっていない。
  - サードパーティのサービスレベルアグリーメント（SLA）がない、またはあいまいである。
  - 重要な連絡用のテンプレートがない。
- 組織的なサポートや賛同が不足している。
  - プランスポンサーに適切な権限がない。
  （例：エグゼクティブ・リーダーシップ・チーム、CIO、CTO、CISO）
  - インシデントに関連する担当者が計画が存在することを知らない。
  - 一事業部門が一方的に計画を作成した。
  - テクニカルチーム以外の部門・担当の役割と責任があいまいである。
- CIRTがメンテナンスされていない。
  - インシデントや演習の教訓が記録されず、遂行されていない。
  - 役割や責任が割り当てられているチーム・個人の連絡先情報がない、または古い。
  - サードベンダーの契約条件が不明、または定義されていない 。

2.インシデント対応計画で重要な要素とは何ですか？

セキュリティインシデントに備えるか否かは、言うなれば嵐に直面しても平穏にすごせるか、またはとんでもないの大混乱になってしまうのか、雲泥の差にあります。主要な考えを踏まえ、CIRP を構築・維持しておきましょう。

Secureworks

システムと情報分類のガイドライン

被害を受けた資産の重要性レベルを、迅速に特定できるように体系的に方法を確立することは、インシデントに適切なレベルで対応するために重要です。システムと情報の分類は、インシデントの優先順位の割当て、リスク重大度の評価、範囲の拡大、通知する関係者の特定、封じ込め、根絶、復旧のための最善の行動指針の決定を行う上での要素として使用されます。

インシデント対応

セキュアワークスのインシデント対応プラクティスは、包括的で認定済みのインシデント対応機能を提供するため、幅広いサイバー攻撃シナリオに備えて対応し、サイバー・インシデントを効率的かつ効果的に軽減することができます。セキュアワークスは、長年にわたるサイバー攻撃と脅威グループのデータに裏打ちされた独自の最新脅威インテリジェンスと専用のテクノロジーを活用することで、最も複雑で大規模なセキュリティインシデントであっても、お客様の準備・対応・復旧をサポートします。

インシデントの優先順位付け：
インシデントはすべてが同じではありません。インシデントの対応が、脅威の内容と関係する資産の重要性に対して適切であることが重要です。優先順位付けは、インシデントのトリアージを行う際の重要な事項であり、ほとんどのインシデント対応チームにとって限られているリソースを、効果的に使用することができます。優先順位付けは、単に定義された脅威モデルや想定されるインシデントタイプのリストに優先度を振りわけるだけではありません。関係する資産、その資産への潜在的リスク、およびその資産がサポートするビジネスへの潜在的なリスクを理解する必要があります。インシデントの優先度を定義するには、上記の分類ガイドラインに加え、インシデント、脅威、影響、緊急度の分類を定義する必要があります。

レスポンスチームの決定と権限付与：
インシデントへの対応者が、特定の権限と機能に対処するためのリソースを迅速に決定することは重要です。役割と責任は、コンピューターセキュリティインシデント対応チーム（CSIRT）の構造の定義からはじまり、通常、シニアリーダー、コアチーム、拡張チーム、外部チームの４つと定義されます。テクノロジーグループやセキュリティグループだけでなく、組織全体を組み入れることが必要です。この計画は、法務、財務、広報、コミュニケーション、人事などのグループに特定の役割と責任を割り当てる構造に基づいています。さらに、この役割と責任は、通知プロセスとエスカレーション・プロセスの作成、コミュニケーション計画の編成、対応の運用テンポの設定、また、行動する役割や決定責任を負う役割を指定する際に使用されます。行動には、インシデントの公表、外部弁護士の呼び出し、法執行機関との連携、電子証拠開示の管理、フォレンジックの実施、潜在的な証拠の保全が含まれます。同様に、決定事項には、ネットワークの一部分離、重要なシステムのサービスからからの隔離、システムの再構築あるいは分析のための保存、サードベンダーへのサポート依頼などを行うタイミングが含まれます。

Secureworks

特定の応答プロセス：
チームメンバーとその役割や責任を決定することは重要ですが、次の手順は、予測可能でかつ再現可能な共通のプロセスを確立することです。

このプロセスは、簡単なチェックリストから詳細なプレイブックまで様々で、通常、「何をするべきか」をカバーし、主要なインシデントタイプごとに作成する必要があります。これらのプロセスは万能ではありませんが、インシデントの規模や範囲に関係なく、実行される一般的な思考プロセスと手順は同じです。これらのプロセスを文書化することで、適切な手順が検討され、必要に応じて実行されるようになります。

インシデントガイド（「何をするべきか」を特定する）は、標準操作手順（SOP）のような、「何かを行う方法」をとは異なります。インシデントガイドで SOP を参照することは珍しくありません。インシデントガイドは主要なインシデントタイプごとに作成され、タスクをチームや個人に割り当てるよう対応チームに指示する必要があります。

CIRPの検証：
データのバックアップと同様に、CIRP が機能するかどうかを確認する唯一の方法は、演習中またはインシデント中にデータをテストすることです。またこれもバックアップと同様に、CIRP がテストされていない場合は、CIRP が十分に機能しないと想定するのが最善です。

以上の要素がすべて準備できたら、きっと問われるであろう「またデータ漏洩のニュースがあった。もしうちで起こったら、準備は大丈夫か?」というリーダーからの質問にも答えることができるでしょう。

3. インシデント対応プロセスにリーダーをどうやって巻き込めばればよいですか？

CIRP を使用することには多くの利点がありますが、全体的な目的は、インシデント中の損害を抑制または回避しながら、調整と意思決定を改善することにあります。インシデント中の効果的な調整は、多くの内部グループだけでなく、外部グループ（主要ベンダー、法執行機関、外部弁護士、保険ブローカー、およびフォレンジック専門家）にも及びます。CIRP は、様々なグループ間の関係を維持し、期待値を設定して、通信プロトコルを導き、グループ間の活動を明確に説明し、CIRP テストの参加を奨励するのに役立ちます。

インシデントが発生すると、通常の動作が中断されるのは事実です。ビジネスへの影響を抑えるために、速やかな対応と、多くの場合迅速な意思決定が必要になります。意思決定の権限者と、その決定を実行する責任者が誰なのかを把握しておくと、CSIRT では、技術的な問題への対応に集中することができます。また、ひとたび責任が割り当てられると、そのチームや個人は、責任を実行するための段階的な手順の構築と適合を開始するため、業務はさらに改善されます。

サイバーセキュリティのインシデントに起因する被害は、多くの方法で測定することができます。対応と修復に必要な時間、サービス停止の期間、SLA を満たしていないために滞った支払い、消費者の信頼の喪失、株価の低下（上場している場合）、罰金（規制に反した場合）などです。損害には、対応するための外部サポートの費用と訴訟の費用が含まれる場合があります。CIRP は、組織の技術的および非技術的対応の取り組みを導き、インシデントがエスカレートするリスクを軽減し、規制上の要件を果たし、デューデリジェンスを実証することで、損害を軽減することができます。

4. ログの記録を効果的に確認する戦略を教えてください。

ログ記録の戦略をしくじると、組織が漏洩後に何が起こったのかを把握できません。多くの場合、PCI-DSS などのコンプライアンス基準で義務付けられているログ記録に関連する戦略が既にあるはずです。一般的に、ネットワーク境界ログとシステムログに簡単にアクセスでき、それらのログを確認できるように一元化しておく必要があります。

通常、セキュアワークスが必ず確認するものには、ログインとログオフ（セキュリティイベントログ）に関するデータを、少なくとも 3 か月前、可能であればもっと前まで遡って確認します。次に、日付、時刻、ソース IP アドレス、ユーザーアカウント、その他のコンテキスト（ログオンの成功や失敗など）を含むシステムへのリモートアクセスの記録も確認します。Web ログや、ファイアウォール、NetFlow、AV ログも重要です。

しかし収集しすぎてしまう問題があります。例えば、あるお客様は、サーバーのセキュリティイベントログにすべてのファイアウォールアクティビティを収集していました。データは非常に広範囲で、45 分ごとにロールアウトされていました。セキュアワークスが依頼を受けて侵入を調査した時に、ネットワークのログイン記録（セキュリティイベントログに含まれる最も有用なもの）を確認したかったのですが、たった 45 分間分のデータしか残っておらず、役に立ちませんでした。

5. 組織がインシデント対応でやってしまいがちな「3 つの間違い」とは何ですか？

漏洩が発生して組織が対応しなければならなくなったときに、計画自体に欠けている点があると問題を引き起こしやすくなります。まず当社の経験から、オフィスとインフラストラクチャが分散している組織では、セキュリティインフラストラクチャの集中管理ができていないことがあります。この分散型のアプローチは、役割や責任、方針が組織全体で明確に定義や理解されていないため、どんな効果的な対応もうまくいきません。第 2 に、ほとんどの組織のインシデント対応計画は更新やテストが実施されておりません。最新ではなかったり、不完全だったり、テストされていない IR 計画をよく見かけます。第 3 に、組織が十分なログを保存しないと、フォレンジックの時間が長くなり、役に立たなくなってしまいます。組織は、少なくとも 1 年間は、Active Directory、DHCP、ファイアウォール、DNS、およびその他のログを収集して集中管理する必要があります。すぐにアクセスできるため、フォレンジックアナリストの負荷が軽減されます。

Secureworks®

セキュアワークス（NASDAQ:SCWX）は、デジタルで接続された世界で組織を保護するサイバーセキュリティのリーダーです。

当社は、何千もの顧客からの可視性を統合し、あらゆる場所のあらゆるソースからデータを収集して分析し、セキュリティ侵害の防止、リアルタイムでの悪意ある活動の検出、迅速な対応、そして新たな攻撃の予測を行います。当社は、お客様に「知識を集めて、もっとずっと安全な（Collectively Smarter. Exponentially Safer.™）」サイバー防御を提供します。

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

日本
〒212-8589
川崎市幸区堀川町580
ソリッドスクエア東館20階
03-6893-2317
www.secureworks.jp