インシデントレスポンスガイド

準備

- 貴組織の上級管理職およびその他の関連職員と協力して、サイバーリスクアセスメントにおいて特定された最も差し迫ったリスクに基づくインシデントレスポンスおよび事業継続性計画を策定する。
  - 貴組織において最も優先度の高いサイバーリスクに関わるインシデントの種類に対応した脅威シナリオを策定する。こうしたシナリオに対応できるキャパシティの構築に焦点を当てること。
  - インシデントレスポンスに関する連絡先リストを特定および記録し、組織内で提供する。
  - 関連する地方自治体および連邦の法執行機関および当局者に関する連絡先情報を特定・記録する。
  - どのような種類のインシデントをいつ、誰に通報する必要があるのかを明記した条項を設ける。
  - インシデントが及ぼす機能および情報面での影響、またそこからの復元可能性などの関連要素に基づき、職員に求められるインシデントレスポンスの速さ、また職員が実行するべき行動を概説した書面上のガイドラインを設ける。
  - 全ての従業員に対し、インシデントが発生した場合は技術チームに連絡するよう伝えておくこと。一般的に、これはITスタッフおよび／または CISO／CIO／その他の同等マネージャーが該当する。
  - ソリューションを展開して、従業員の行動を監視し、内部脅威およびインシデントの特定を可能にする。
  - 事業継続性計画を含めることで、貴組織が業務上の緊急事態に遭遇した際はサプライヤーおよび主要顧客とどのように協働するのか調整する。これには、必要に応じて手動または代替の事業運営の実施方法を含める。
  - 緊急システムの停止および再起動に関する書面上の手順を含める。
  - バックアップデータの回収および復元用のテスト手法を開発する。定期的にバックアップデータをテストして、その妥当性を検証する。
  - 代替の施設／現場で事業活動を行うための確立した合意および手順を用意する。
  - 全ての顧客を対象とした明確な普及チャンネルを配備する。

演習

- 全ての職員または組織の重役、PR／コミュニケーション職員、および法務・コンプライアンスチームを含む、あらゆる職位の代表者と共に小規模な机上演習を編成する。
- 貴組織に関連性のある、業界全土の机上演習を特定して、可能な限り参加する。
- 演習で学んだ教訓を貴組織のサイバーセキュリティ戦略に確実に取り込むための プロセスを設定する。

レスポンス

- 風評被害を含む、事業活動に対する影響を最小限に留めるため、インシデントレスポンス計画の行動を実装する。
- 影響／被害を受けたシステムを特定して、その損害を評価する。
- 影響を受けたアセットを取り除き（接続を解除）、損害を減らす。
- チームがインシデントの発生を疑った時点で、早急にあらゆる情報の記録を開始する。影響を受けたことが特定されたアセットの接続解除／隔離を行いながら、インシデントの証拠保全を試みる（例：影響を受けたログのシステム構成、ネットワーク、侵入検知ログの収集）。
- 適切な内部当事者、第三者ベンダー、および当局に通達して、必要ならば支援を要請する。
- 法規および関連機関のガイダンスに沿った形で顧客への通知および支援活動を開始する。
- FS-ISAC または MISP などの脅威情報共有プラットフォームを利用して、脅威に関して業界に通達する。
- 後日見直すことができるよう、インシデント中に取った全てのステップを文書化する。

復元

- 可能であれば回収したアセットを定期的に「リカバリポイント」で復元して、最後に確認された「良好」ステータスにバックアップデータで復元する。
- 復元したアセットから最新の「クリーン」なバックアップを作成して、重要なアセットの全てのバックアップを物理的および環境的にセキュアなロケーションに確実に保管する。
- 感染したシステムが完全に復元したことをテスト・検証する。 影響を受けたシステムが正常通り機能していることを確認する。

審査

- インシデント発生後は「学んだ教訓」に関するディスカッションを実施する。上級職員、信頼できるアドバイザー、そしてコンピューターサポートベンダーと会い、予想される脆弱性の審査または実装すべき新たなステップの推奨を行う。
- 可能であれば、インシデントを引き起こした脆弱性を特定し（ソフトウェア、ハードウェア、事業活動、または従業員の行動において）、これを緩和する計画を立てる。
- 特定した問題に関連した類似または将来的なインシデントの検出を可能にする監視計画を策定する。
- インシデントの情報および学んだ教訓について、FS-ISACなどの脅威情報共有プラットフォームで共有する。
- 学んだ教訓を貴組織のインシデントレスポンスプロトコルに取り込む。