サイバーレジリエンスに関する8つのベストプラクティス

攻撃を受ける前に、自信を持って計画を実行に移します。

概要

災害復旧計画が策定されていても、破壊的なサイバー攻撃からの復旧には別のアプローチが求められます。それは、セキュアに復旧するためには、迅速な対応、攻撃の発生経緯に関する効果的な調査、脅威の軽減を実現する必要があるためです。

次の8つのベストプラクティスに従うことで、真のサイバーレジリエンスに向けて前進することができます。

1. 万全の準備

まずは、全関係者を含む、部門横断型のランサムウェアレジリエンスチームを発足します。ランサムウェアインシデントは組織全体に影響を及ぼすため、サイバー攻撃を受けている間に全員が自分の役割を把握していることが重要です。全関係者を含めた現実的な机上演習の実施、組織全体のランサムウェアポリシー の作成 (および定期的な更新)、サイバー攻撃に備えたバックアップと運用レジリエンス戦略の策定を検討します。

2. 先手を打つ対策

所属する業界や地域で収集したインテリジェンスを活用し、ランサムウェア攻撃者と、彼らが用いるツール、手法、手順 (TTP) について理解します。対応チームの全メンバーの連絡先情報を文書化して保管し、攻撃の影響を受けない領域外のコミュニケーションチャネルでやり取りをするのが理想です。ランサムウェアのような挙動を報告するためのチャネルを作成します。サイバー危機対応チームを編成し、必要に応じてインシデント対応組織のサービスを利用します。

3. 攻撃対象領域の縮小

重要資産の脆弱性を特定し、パッチを適用します。重要なシステムと、ランサムウェア集団に用いられる攻撃ベクトルを優先して、システムを強化します。全システムの資格情報とアクセス権限が最小権限の原則に基づいて管理されていることを確認します。ランサムウェアの拡散を抑え、ラテラルムーブメントを検知できる可能性を高めるため、ネットワークのセグメンテーションを行います。また、組織内にある、機密データを含みながらもセキュリティが不十分なデータリポジトリを特定します。

4. バックアップの保護

バックアップシステムが十分にエアギャップされ、職務が分離され、攻撃者による破損や削除を防ぐイミュータブルデータストアを利用していることを確認します。バックアップ管理者に対する多要素認証 (MFA) と、ロールベースのアクセス制御 (RBAC) を利用します。再構築を加速するため、重要システムのゴールデンマスターを作成して保管します。また、バックアップシステムが、ランサムウェアインシデントの対応に必要なサイバーセキュリティ機能に対応できることを確認します。

5. ランサムウェアに対する保護の強化

ランサムウェア集団が用いるATT&CKの手法に対する、既存の予防・検知制御の適用範囲におけるギャップを特定します。ランサムウェアやワイパー攻撃に関連する、ファイルの暗号化や削除といったエンドポイントのファイルシステムの異常を検知できるようにします。既知の悪意ある指標を含むメールをブロックするよう、メールゲートウェイフィルターを導入します。承認されたソフトウェアのみが実行されるよう、重要資産のホワイトリスト機能を備えたアプリケーションを使用します。

6. ランサムウェアに対する検知の強化

侵害を検出するため、履歴データを活用して積極的にハンティングを実施します。CPUやディスク使用率の異常な変動を検知する仕組みを導入します。I2PやTORなど、ランサムウェア集団が使用することで知られる異常なネットワークプロトコルを特定します。また、ランサムウェアやワイパーのコマンド & コントロールで使用される既知のポートや送信先を用いて、ネットワーク接続を特定します。

7. インシデントへの対応

影響を受けた資産に関連する類似のアラートを特定し、グループ化します。以下を含む、インシデントの初期損失予測 (影響範囲) を作成します。データ窃取に使用されたステージング環境を特定し、有線と無線ネットワークの両方から感染しているホストを隔離します。クリーンルームの有効化、影響を受けたシステムの最終バックアップのクリーンルーム環境へのリストア、クリーンルーム内のシステムに対する信頼できる検知/応答ツールの再展開を実施します。永続性の証拠を探し、攻撃で悪用されたシステムの脆弱性を特定します。

8. コミュニケーション

内部関係者、有害な憶測を防ぐための報道機関、規制上や法律上の義務に基づいた通知が必要となる影響を受けるデータ主体、規制当局に対して連絡を行います。保険会社、法執行機関、国や業界のCERTに通知します。

各ステップの詳細については、ホワイトペーパーをお読みください。

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

9100083-001-JP 4-2025