ランサムウェア：防止および保護

リアルタイム保護

悪意のある行為を行うものがコンピューターシステムを麻痺させ、元に戻すため身代金の支払いを要求することで、マルウェアによる収益化手段を見つけて以降、ランサムウェアの脅威は増大し続けている。効果的に運用させるには長期にわたって隠しておく必要のあるその他のマルウェアとは異なり、ランサムウェアはスピアーフィッシング、不正アクセスを受けた Web サイト、そして破損したダウンロードによって迅速に実行できるようエンジニアリングされている。金融機関は、ランサムウェアの影響を特に受けやすくなっている。これは、魅力的な標的と見なされている以外にも、資金を迅速かつ効率的に動かす能力が脅かされることが原因となっている。しかし、悪意のある行為を行うものは、必ずしも約束を守る訳ではない。身代金の支払いを得ても、マルウェアの除去や機密データへのアクセス制限解除を行わない攻撃者も存在する。

- 新たな脅威インテリジェンスにリアルタイムで適応できるアンチマルウェア保護システムに投資する。
- 機密または必須情報を収容したネットワークに接続した全てのデバイスのセキュリティを評価する。必須ではない全てのシステムを別のネットワークに接続する。
    - 職場にIoTまたは「スマートデバイス」を持ち込む際は、特に注意が必要である。なぜなら、こうしたシステムのセキュリティは脆弱であるか、ほぼ存在しない場合が多いため、必須システムへのアクセスポイントとして標的にされる可能性があるため。
    - リモートワークセットアップのセキュリティを考慮する。セキュリティツールがオフネットワークでも動作し、全ての Web トラフィックを監視できるようにする。
- フィッシング攻撃および強力なパスワード保護の必要性に関して従業員教育を推進する。
- 実行可能であれば、組織全土における多要素認証の実装を検討する。
- 全てのソフトウェアおよびシステムを定期的にアップデートする。可能であれば、自動アップデートに設定を変更する。
- ランサムウェア攻撃および貴重なデータの損失に対処するためのインシデントレスポンスおよび危機管理計画を策定する。
- ランサムウェア攻撃が発生した場合に備えて外部コミュニケーション計画を準備する。

データバックアップ

- データを常に保護する、セキュアかつ定期的にアップデートされるバックアップシステムに投資する。
    - USB またはハードドライブを利用する場合は、バックアップの終了後にネットワークコンピューターからこうしたデバイスの接続を物理的に切断する。
    - クラウドストレージを利用する場合は、サーバーに高レベルな暗号化と多要素認証を配備する。
- 最悪の場合のディザスタリカバリに備えて、総勘定元帳の読み取り専用コピーを作成しておく。
- 自動データリカバリおよび修復を実行するシステムを開発する。
- 重要データおよびビジネスサービスの復元にどの程度の時間を要するか、シナリオを策定する。

規制環境

- 運用環境におけるランサムウェアに関する法規ガイダンスを評価する。
    - 各国ごとのガイダンスを考慮する。変更されたガイダンスの定期的な評価計画を策定する。
    - 金融セクター固有のガイダンスを考慮する。
    - 国際的な法規要件を考慮する。
- 身代金を支払う場合のリスクを評価する。一部のケースでは、身代金の支払いが悪意のある行為を行うものに対して配備された既存の制裁体制への違反となる場合がある。
- 現地法執行機関と連絡を取る。攻撃が発生した場合の迅速な情報共有のつながりを築く。
- ランサムウェアに関するサイバー保険ポリシーのメリットとデメリットを評価する。

組織のランサムウェアに対するレディネスの測定

ランサムウェアの防止および保護対策を策定する際は、以下の質問を検討すること。

1. 貴組織では、**定期的なスケジュールバックアップ**を実施しているだろうか？
    - こうしたバックアップは、クラウドストレージシステムまたはエアギャップされた USB／ハードドライブ経由で接続を遮断されているだろうか？
2. 貴組織のネットワークには、**必須でないデバイス**が接続されているだろうか？
    - こうしたデバイスは、機密データを収容していない他のネットワークに移動できるだろうか？
3. 貴組織は、身代金の支払いに伴う**法規上のリスク**について把握しているだろうか？
    - この点に関する法務ガイダンスは国ごとに異なり、頻繁に更新されている。
4. 貴組織は、ソフトウェアおよびシステムを定期的にアップデートしているだろうか？ こうしたアップデートは**自動化**されているだろうか？
5. 貴組織は、**ランサムウェア攻撃およびデータ損失に対処するための計画**を抱えているだろうか？
6. 貴組織は、**サイバー保険ポリシー**に加入しているだろうか？ ポリシーがある場合、ランサムウェア攻撃はどのように補償されるだろうか？
    - 一部のプランは身代金の支払いを明白に禁止しているほか、中にはポリシーの一環としてこうした支払いを補償するものもある。