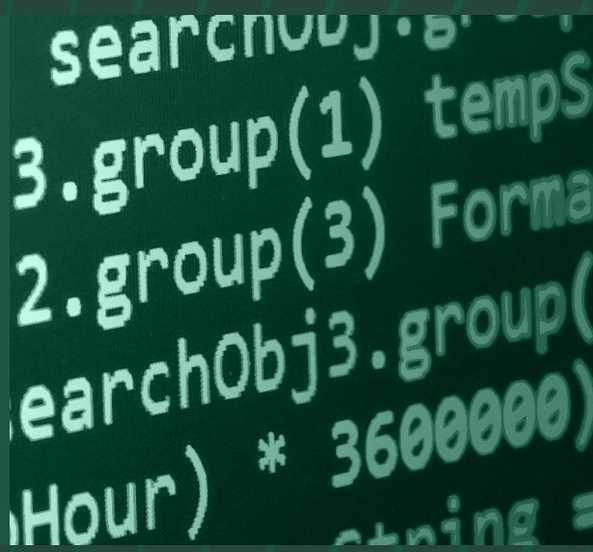
DELL Technologies

5 ランサムウェア攻撃を生き延びるための推奨事項



1 包括的なインシデント対応計画を維持する

- 攻撃の影響を最小限に抑えることに重点を置く
- 頻繁に練習、テスト、アップデートを行う
- インシデント対応チームを事前に準備しておく
- 全体的なレジリエンス戦略の一部としてサイバー保険を検討する
- 法執行機関と協力する計画を含める

2 明確なコミュニケーション戦略を策定する

- コミュニケーション テンプレートを事前に作成する
- 適時かつ明確な組織内コミュニケーションを保つ
- 該当する場合は、外部とのコミュニケーションに備える
- 適用される通知規制を遵守する

3 データ保護を堅牢に保つ

- 隔離された不変のエアギャップ データ ヴォールトで重要なデータを保護する
- サービス/インフラストラクチャごとにリカバリーの優先順位を付ける
- リカバリー可能性を実践する
- クリーン ルームなどの機能を目標リカバリー時間と組み合わせる
- リカバリー可能なデータの完全性を確保する

4 すぐに正常に戻ると思い込まない

- 身代金の支払いは最後の手段にすべき
- 支払う前に、法的および規制要件へのコンプライアンスを確保する
- 身代金を支払っても、ハッカーがデータを返すという保証はない

5 トレーニングと教育を重視する

- 攻撃シミュレーションを実施する
- セキュリティ ハイジーンに関する従業員の慣行を監視およびテストする
- フィッシング テストやEメール セキュリティ トレーニングなどのツールを使用する

もはや「もし」ではなく「いつ」が問題になっている

企業は、最善の防御策を講じていても、攻撃は避けられないものとして計画を立てる必要があります。Dellの特定分野の専門家であるJim Shook（サイバーセキュリティおよびコンプライアンス プラクティス担当グローバル ディレクター）とSteven Granat（サイバーセキュリティ ソリューションおよび戦略的パートナーシップ担当主席コンサルタント）が、Brian White（Dell Data Protectionのプロダクト マーケティング部門シニア コンサルタント）と災害発生時の対応について話し合いました。

> 適切な人材を招いてトレーニングを行い、アクションをシミュレートして、攻撃が発生したときに、誰もが自分が何をしているのかをすぐに把握できるようにしておく必要があります」
>
> ***Steven Granat**、デル・テクノロジーズ、*
> *サイバーセキュリティ ソリューションおよび戦略的パートナーシップ担当主席コンサルタント*

包括的なインシデント対応計画を維持する

攻撃が発生した場合、すべての主要なステークホルダー（組織内のほぼ全員、サプライヤーなどのサード パーティーも含む）は、何をすべきかを知っておく必要があります。インシデント対応計画に一連の行動を明確に記載しておく必要があると、Shookは助言します。包括的な計画では、即時の対応からリカバリーに至るまで、技術、プロセス、コミュニケーションに関わる手順を取り扱います。デジタル通信モードが機能しない可能性があるため、紙ベースの文書も必ず常備してください。「文字どおり、棚に行って取り出せるような計画書が必要です」とGranatは言います。

明確なコミュニケーション戦略を策定する

ほとんどの組織は、主要なステークホルダーとコミュニケーションをとる必要があり、多くの場合、規制要件に準拠する必要もあります。社内外のコミュニケーション用にさまざまなテンプレートを作成し、誰にどのような順序でいつ通知するかを体系的にまとめておきます。電話やEメール システムがダウンした場合に備えてください。

堅牢なデータ保護戦略を実施する

ランサムウェア攻撃をしのぐための重要な目標は、身代金を支払わずに、できるだけ痛みを伴わずにデータをリストアしてリカバリーすることです。強力なデータ保護戦略は、こうした目標を達成するための重要な部分ですが、テクノロジーとプロセスの両方を含める必要があります。「不変データとサイバー ヴォールトを使用して信頼できる十分なデータを保存するか、少なくともシステムのリカバリーを可能にする検証ポイントとして不変データとサイバー ヴォールトを使用してください」とShookは助言します。データを確実に保護することが最初のステップです。また、リカバリーするための人材とプロセスも用意する必要があります。支援を仰げるサード パーティーの専門家もいますが、計画段階で参加してもらう必要があります。

身代金を支払っても、すぐに正常に戻ると思い込まない

身代金の支払いは最後の手段としてのみ検討されるべきであり、すぐに平常業務の再開が保証されるわけではありません。犯罪者と交渉していることを忘れないでください。たとえデコーダー キーを入手したとしても、新たに復元されたデータに対して戦略を立てておく必要があります。まず、復号化されたデータをテストし、すべてのシステムを系統的に再構築する必要があります。攻撃が発生する前でも、起こり得る事態に対して繰り返し細心の注意を払うことは、レジリエンスの向上に大いに役立ちます。「技術インフラストラクチャ内のさまざまなアプリケーションと依存関係を理解することは、平常状態に効率的に戻るために不可欠です。実行可能なリカバリー ソースとリカバリー可能なターゲットはあるか？侵害を受けていないデータはあるか？これらは検討すべき重要な事項です」とGranatは言います。

リカバリー段階では、攻撃者が本当にシステムから立ち去ったことを確認する必要もあります。「家の中で火が消えたことを確認し、そもそも何が火事の原因になったのかを突き止める必要があります。この2つの重要な情報がなければ、将来の攻撃に対して無防備になってしまうからです」とShookは言います。

トレーニングと練習が重要

サイバー レジリエンスの重要な部分は、包括的なトレーニングです。これは、従業員が強力なサイバーセキュリティ ハイジーンを実践することから、リカバリー計画を日常的に実践することまでを含みます。「適切な人材を集めてトレーニングを行い、アクションをシミュレートして、攻撃が発生したときに、誰もが自分が何をしているのかをすぐに把握できるようにしておく必要があります」とShookは言います。

今日の脅威ランドスケープにおいて、ランサムウェアは避けられないものかもしれませんが、計画と実行を通じて、事業、財務、評判への影響を最小限に抑えることができます。目標は、できるだけ早く、痛みを伴わずに通常の状態に戻ることです。

dell.com/cybersecuritymonthで今日のサイバーセキュリティの重要な課題に対処する方法をご紹介しています

DELL Technologies