COMMVAULT

ランサムウェア：保護とリカバリのための 4 つの方法

データへのアクセスにビジネスが依存している場合、最優先は高速なリカバリ

サイバー セキュリティ専門家の警告どおり、2017 年はランサムウェアによる不正な攻撃が増加しています。残念ながら、ランサムウェアのたくらみはサイバー犯罪の容易な収入源となり、それにより毎年攻撃の件数が増え続けています。攻撃されると、保護されていない組織は重要な電子ファイルにアクセスできなくなり、ビジネス全体がリスクにさらされます。組織は、データへのアクセスを取り戻すため、ファイルが本当にリリースされることを願って身代金の支払いに応じたり、現在のデータを確実に再現できる保証がないにもかかわらず、一時しのぎのリストアを試みたりします。重要なデータへ常にアクセスできるようにしておくために、ランサムウェアの攻撃から確実に保護、リカバリできるよう、次の 4 つのベスト プラクティスを検討してください。

ランサムウェア攻撃からの保護とリカバリのための 4 つの方法

複数層のセキュリティ戦略 (マルウェア対策、パーソナル ファイアウォール、ハード ディスクとファイルの暗号化、DLP など) の実装は、増大するサイバー セキュリティの脅威から保護するために不可欠です。ただし、これらのすべてのエンドポイント保護ソリューションをもってしても、そこには依然としてそこそこの脅威があります。Gartner の「エンドポイントの保護プラットフォームに関するマジック クアドラント」[1] によれば、「EPP (エンドポイント保護プラットフォーム) ソリューションのレファレンス カスタマーの 44% が感染している現状では、悪質な感染をブロックするというその業界の主要目標に失敗していることは明らかです」。

どんなにデータ集約型のビジネス環境であってもランサムウェアから保護するには、次のベスト プラクティスを検討してください。

1: 効果的な情報セキュリティ プログラムを導入する

組織が情報セキュリティに関する経験がないか、または情報セキュリティ機能を部分的に導入したばかりである場合は、表 1 に示した手順に従って、効果的なセキュリティ プログラムの導入を検討してください。

ステップ	アクション
重要なデータがどこに保管されているのかを知る	データの場所を気にし続ける • データセンター • リモートの施設 • クラウド • サービス プロバイダー
在庫システム	• どのシステムが重要なデータを扱っているのかを知る : 保存、処理、転送 • データの流れについて理解する • どのシステムが業務にとって最も高いリスクを与えるのかを判断する
リスクを評価する	• 主要なシステム、サービス、またはデバイスの電子記録、物理メディア、可用性を含める
セキュリティ コントロール策の適用	• リスクに基づいてセキュリティ コントロールを選択、適用、管理します。
効果を監視する	進化する脅威に対して備える • リスクベースの情報セキュリティ戦略、適用済みのセキュリティ コントロール、セキュリティ技術の適切な実装の効果を積極的に評価する • 是正措置、改善、得られた教訓を適用する
ユーザーを教育する	• 不明な送信者から、疑わしい添付ファイルやリンクが含まれたメールを受信したときにどうしたらよいか、確実に従業員を教育する (推奨の手順については付録を参照ください)

表 1: 効果的な情報セキュリティ プログラムの要素

ランサムウェア: 5 つの主なタイプに対する防御

受けているランサムウェア攻撃のタイプを知っておくと、その初期対応で発生する損害を大幅に抑えることができます。

今すぐ読む

PDF commvau.lt/2s3JUHV

1 Gartner 「エンドポイント保護プラットフォームのマジック クアドラント」2016 年 2 月 1 日

2: 技術的ベスト プラクティスでデータを保護する

脅威が増大し、攻撃がさらに高度化している中で、企業はサイバー セキュリティと従業員教育への投資額と、重要なデータにアクセスできなくなることによるビジネスへの影響度とのトレードオフについて明確に理解する必要があります。

ネットワーク セキュリティは、ランサムウェア攻撃に対する最初の防御として優れています。また、効果的な技術的ベスト プラクティスを導入することで、組織はデータと IT インフラストラクチャをさらに保護できます。表 2 に、ランサムウェア攻撃による感染の可能性を排除するための主要な技術戦略を示します。

ステップ	アクション
検出と防止	多角的なセキュリティ ソリューションを採用する • 関連するパッチでシステムとソフトウェアを常に更新し続ける • ファイル ベースの脅威 (従来の AV) に対する保護、ダウンロードの保護、ブラウザーの保護、発見的技術、ファイアウォール、コミュニティーからのファイル評価スコアリング システム
外部の CERT グループ (コンピューター緊急事態対策チーム) を利用する	• ウイルス ソフトウェア会社より先に問題を発見することがよくある • 手動フィルタリングのための緊急措置について推奨することができる (ソフトウェア会社はパッチのリリースに数時間または数日を必要とする可能性がある)
感染の特定と停止	包括的な防止ポリシーを定める • エンドポイントとネットワークのポリシーと、ウイルス対策、スパイウェア対策、ファイアウォール タイプなどの保護製品を含める • ワークステーションで承認されていないプログラムの実行を制限する • エンド ユーザーの書き込み権限を制限し、たとえそれらがランサムウェア アプリケーションをダウンロードして実行した場合でも、そのユーザーの特定のファイル以外のファイルを暗号化できないようにする • 重要なシステム、サービス、またはデバイスの電子記録、物理メディア、可用性を含める
システムと構成の “ゴールド” イメージを持つ	• データ管理ポリシーの基本的な要素 • マスターで、感染したシステムのクローンを簡単に作成する
包括的なバックアップ戦略を保持する	• バックアップは、重要なファイルへのアクセスを取り戻すための最も高速な方法です • ボリューム レベルのスナップショットをより頻繁に (15 分ごとに) に作成し、それをより長期間保存しておきます。 • 影響を受けたシステムをネットワークから切断し、脅威を取り除きます。 • 影響を受けたファイルを、問題がないことがわかっているバックアップからリストアします
効果を監視する	進化する脅威に対して備える • リスクベースの情報セキュリティ コントロール、適用済みのセキュリティ管理策、セキュリティ技術の適切な実装の効果を積極的に評価する • 是正措置、改善、得られた教訓を適用する
ユーザーを教育する	• 不明な送信者から、疑わしい添付ファイルやリンクが含まれたメールを受信したときにどうしたらよいか、確実に従業員を教育する (推奨の手順については付録を参照ください)

表 2: 技術的ベスト プラクティス

3: 効果的なバックアップ戦略を採用する

ほとんどの場合、ランサムウェア イベントは進行性のハッキングであると認識してください。時間をかけて動作し、1 週間またはそれ以上バックグラウンドで実行されて、お客様のバックアップ ルーチンの動作を学習します。そのため、ディザスタ リカバリ手順の一環として、データのコピーを永続的に他の場所に保持することが重要です。

バックアップとしてスナップショットのみに依存する多くの企業は、高いリスクにさらされています。スナップショットまたは他のインスタンスを複製すると、複製に基づいているソースも壊れます。保護された場所に、以前のリカバリ ポイントから温存したバージョンのデータを持つことが鍵になります。

ステップ	アクション
バックアップまたは DR プロセスを採用する	• 同じシステムに保存されたバージョンではなく、バックアップ コピーを直接呼び出します。 • ソース システムに保持した単なるスナップショットだけでなく、データのバックアップ コピーを外部に持ちます。

表 3: データ保護のベスト プラクティス

クラウド ライブラリの使用は、きちんと外部にデータを集めておくことの代替策となります。クラウド バックアップはローカル管理者のオペレーティング システム アカウントには見えないため、クラウドのユーザー認証情報へアクセスするには、さらに高度な知識が必要となります。さらに、" ディスクのみ " の時代においてテープは好まれませんが、ディスクのオンライン性には永続的なリスクがあるため、一部のビジネスにとってはクラウドは優れた代替策となり得ます。

4: エンドポイントの保護について従業員を教育する

最後に、データを扱うすべての従業員に優れたセキュリティ習慣を育することは、ビジネスをセキュアに保つために不可欠です。常識に従って行動するように伝えてください。「インターネット セキュリティ脅威レポート」[2] で示されているように、表 4 に記載のベスト プラクティスについてユーザーを教育します。

ステップ	アクション
セキュリティのベスト プラクティスについてユーザーをトレーニングする	• 想定していたもので、既知の信頼されたソースからのものでない限り、添付ファイルを開かない。 • 信頼されたソースからのものであるか、ダウンロードに対してマルウェアのスキャンを実行した場合を除き、インターネットからダウンロードした (このようなアクションが許可されている場合) ソフトウェアを実行しない。 • 信頼されたソースや友人からのものである場合でも、メールまたはソーシャル メディア プログラム内の URL をクリックするときは注意する。 • 安全なソーシャル メディアの利用を促す。ホット トピックは詐欺の恰好の餌となり、すべてのリンクが実際のログイン ページにつながるとは限りません。 • 何か疑わしいものを見つけた場合は、警告を出すよう従業員に奨励する。 • Windows ユーザーが URL をクリックするか検索エンジンを使用した後に、" 感染しています " という警告が表示された場合は (偽のウイルス感染を示します)、Alt + F4 キー、Ctrl + W キー、またはタスク マネージャーを使用してブラウザーを閉じるか終了し、ヘルプデスクに通知する必要があります。

表 4

2 Symantec「インターネット セキュリティ脅威レポート」Vol 21 、2016 年 4 月

組織でランサムウェア攻撃が発生した場合に事業中断を最小限に抑えるための唯一の方法は、アプリケーション、サーバー、エンド ユーザー マシンをすべて対象とした完全なリカバリ ソリューションです。詳細については、commvault.com/ransomware をご覧ください。

COMMVAULT

COMMVAULT SYSTEMS JAPAN 株式会社　〒141-6008 東京都品川区大崎 2-1-1 THINKPARK TOWER 8F

WWW.COMMVAULT.COM | PHONE: 03-5747-9610 | JPSALES@COMMVAULT.COM