COMMVAULT

WHITEPAPER

ランサムウェア: 保護とリカバリのための4つの方法

私たちはよくランサムウェア攻撃に関するニュースを聞きます。ランサムウェア攻撃は、サイバー ライフの不幸な部分です。悪いことに、これらの犯罪者にとってビジネスは非常に好調で、ますます高度な脅威が発生しています。これにより、組織はデータへアクセスできなくなり、ビジネス全体が危険にさらされる可能性があります。データ保護が十分でない組織は、データが本当に解放されることを "希望" して身代金を支払うことを余儀なくされるか、確実にリカバリできる保証なくその場しのぎのリカバリを試みます。重要なデータへのアクセスを維持するには、4つのベスト プラクティスを考慮し、ランサムウェア攻撃から確実にデータを保護およびリカバリする必要があります。

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

マルウェア対策、パーソナル ファイアウォール、ファイルの暗号化、データ損失防止ソフトウェア (DLP) などを含む多層のセキュリティ戦略を実装することは、増大するサイバー脅威からエンドポイント (ノートPCやデスクトップ) とインフラストラクチャを保護するために重要です。しかしながら、これらすべての保護ソリューションを使用しても、依然、データ攻撃を受ける可能性は残るため、データをバックアップしておくことは大切です。

「別のデバイスにファイルの定期的なコピーを作成しておくことは、サイバー攻撃の被害を最小限に抑える唯一の効果的な方法です。信頼性の高いバックアップがあれば、すべてのファイルを無傷のまま、できるだけ早く、通常のコンピューターの使用状態に戻すことができます」

引用: The Threat Report, Myths In Cybersecurity That People Needs To Forget, 2019

最もデータ集約型のビジネス環境でもランサムウェアから保護できるよう、そのベスト プラクティスを以下にまとめました。

1 効果的な情報セキュリティ プログラムがある

組織が情報セキュリティに不慣れな場合、または情報セキュリティ計画を部分的にしか実装していない場合は、次の手順を実行して効果的なセキュリティ プログラムにすることを検討してください。

表1: 効果的なセキュリティ プログラムのコンポーネント

機能	インテグレーション
重要なデータの保存場所を知る	複雑な環境では、データの保存場所を把握しておくことがこれまで以上に困難になります • データセンター • リモート施設 • クラウド • サービス プロバイダー
インベントリ システム	• 重要なデータを処理しているシステムを把握する: 保存、処理、送信 • データ フローを理解する • どのシステムが運用に最も高いリスクをもたらすかを判断する
リスクを評価する	• 電子記録、物理メディア、主要なシステム/サービス/デバイスの可用性を含める
セキュリティ制御を適用する	リスクに基づいてセキュリティ管理策を選択、適用、管理する
効果を監視する	進化する脅威の状況に備える • リスク ベースの情報セキュリティ戦略の有効性、適用するセキュリティ管理策、セキュリティ技術の適切な実装を事前に評価する • 是正措置、改善、学んだ教訓を適用する
ユーザーを教育する	従業員が、知らない送信者から、疑わしい添付ファイルまたはリンクを含む電子メールを受信した場合の対処方法について教育されていることを確認する (推奨手順については付録を参照)

2 テクノロジーのベスト プラクティスでデータを保護する

脅威の増加と攻撃の高度化に伴い、企業は、サイバーセキュリティと従業員教育への投資のコストと、重要なデータへのアクセスの損失と、その結果発生するビジネスと評判への影響に対するコストについて、そのトレードオフを明確に理解する必要があります。

55% 回答者の55%が、高度な脅威（隠れた、未知の、新興の）の検出がセキュリティ オペレーション センターの最大の課題であると答えました。

Domain Tools
The 2019 Threat Hunting Report

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防御において優れた第一線となります。また、効果的なテクノロジーのベスト プラクティスを実装することにより、組織はデータとITインフラストラクチャをさらに保護することができます。表2は、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の概要を示しています。

表2: テクノロジーのベストプラクティス

機能	インテグレーション
検出と防止	多面的なセキュリティ ソリューションを採用します。 • システムとソフトウェアを関連するパッチで更新し続ける • ファイルベースの脅威（従来のウイルス対策）、ダウンロード保護、ブラウザー保護、ヒューリスティック テクノロジー、ファイアウォール、コミュニティ ソースのファイル レピュテーション スコアリング システムから保護する
外部認証グループを使用する（コンピューター緊急対応チーム）	• ウイルスが企業に感染する前に問題を特定できることが多い • 手動フィルタリングの緊急手順に関する推奨事項を作成することができます（ソフトウェア会社はパッチをリリースするのに数時間または数日かかる場合があります）
感染を特定して停止する	包括的な予防とリカバリ準備ポリシーを定義します: • ウイルス対策、スパイウェア対策、ファイアウォール タイプの製品など、エンドポイントとネットワークのポリシーと保護製品を含む • ワークステーションでの未承認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機能を制限し、たとえランサムウェア アプリケーションをダウンロードし実行しても、ユーザー固有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 • 電子記録、物理メディア、および重要なシステム、サービス、またはデバイスの可用性を含める
システムと構成の ”ゴールド” イメージを保持する	データ管理ポリシーの基本要素: • 感染したシステムをマスターで簡単に複製
包括的なバックアップ戦略を維持する	進化する脅威に備える: • リスク ベースの情報セキュリティ戦略の有効性、適用するセキュリティ管理策、セキュリティ技術の適切な実装を事前に評価する • 是正措置、改善、学んだ教訓を適用する
ユーザーを教育する	従業員が、知らない送信者から、疑わしい添付ファイルまたはリンクを含む電子メールを受信した場合の対処方法について教育されていることを確認する（推奨手順については付録を参照）

3 効果的なバックアップ戦略を採用する

ランサムウェアによるハッキングはほとんどの場合、進行性です。つまり時間をかけて動作し、バックアップ ルーチンの動作を学習しながらバックグラウンドで実行されます。そのため、リカバリ レディネス戦略とディザスタ リカバリ手順の一環として、データの永続的なコピーを他の場所に保持しておくことが重要です。

バックアップとしてスナップショットのみに依存している企業は、より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がレプリケートされると、バックアップ ソースも破損します。きちんと守られている場所に、以前の復旧ポイントから取得したデータ バージョンを持つことは必須です。

表3: データ保護のベスト プラクティス

手順	アクション
バックアップとDRプロセスの採用	• 同じシステムに保存されているバージョンではなく、別のバックアップ コピーを直接呼び出す • ソース システムに保持している単なるスナップショットの他に、外部にデータのバックアップ コピーを持つ

クラウド ライブラリを使用することは、外部にデータを保持しておくための優れた別の選択肢です。クラウド バックアップはローカル管理者のOSアカウントからは見えないため、クラウド ユーザーの資格情報にアクセスするには、機能の高度化が必要になります。誰もテープを愛しているわけではありませんが、ディスクまたはクラウドのオンライン性は永続的にリスクをさらすものであるため、一部の企業にとってはテープがより良い選択肢になるかもしれません。

4 エンドポイント保護のための従業員教育をする

最後に、ビジネスをセキュアに保つには、データに触れるすべての人に正しいセキュリティ習慣を教育することが不可欠です。以下で説明するように、表4に概説されているシマンテックのベスト プラクティスでユーザーを教育します。

表4: 従業員とエンドポイントのベスト プラクティス

手順	アクション
セキュリティのベスト プラクティスを実践するようにユーザーをトレーニングする	• ファイアウォールを使用する • パスワード ポリシーを強化する • コンピューターのプログラムとユーザーが、必要最低限のレベルの権限でタスクを実行していることを確認する • 自動再生を無効にする • 不要なファイル共有をオフにする • 不要なサービスをオフにして削除する • 脅威が1つでもネットワーク サービスを悪用している場合、パッチが適用されるまでそれらのサービスへのアクセスを無効化またはブロックする • 常にパッチレベルを最新に保つ • 脅威の拡散に一般的に使用される添付ファイルを含む電子メールをブロックまたは削除するように電子メール サーバーを構成する • 感染したコンピューターを迅速に分離し、脅威がさらに広がるのを防ぐ • 予期していない添付ファイルを従業員が開かないようにトレーニングする • モバイル デバイスにBluetoothが必要ない場合は、オフにする 詳細は Symantec, Security Best Practice recommendations, 2018 をご覧ください。
エンドポイント保護のベストプラクティスを採用する	• 検索からWebサイトの評価を表示するURLレピュテーション プラグインを導入する • ソフトウェア利用を企業が承認したアプリケーションにのみ制限し、ファイル共有サイトからのソフトウェア ダウンロードを禁止する。信頼できるベンダーのウェブサイトからのみパッケージの直接ダウンロードを行う • 2段階認証をWebサイトまたはアプリに実装する • メール アカウント、アプリケーション、ログインごとにユーザーに異なるパスワードを使用させる – 特に仕事関連のサイトやサービスの場合

結論

重要なビジネス情報を保護することは、どの組織にとっても必須です。そしてその情報をランサムウェアの攻撃から守ることは、あらゆるビジネスにとって最優先事項です。そのため、セキュリティ、テクノロジー、バックアップ、従業員のベスト プラクティスに注意を払うことで、そのデータを保護することが大切です。その結果、データは安全になり、ランサムウェアのリスクを軽減しながら、ビジネスの継続性をより確実にすることが確保できます。

COMMVAULT Be ready™

Commvault Systems Japan 株式会社
東京都品川区大崎2-1-1 ThinkPark Tower 8F
www.commvault.co.jp | 03-5747-9610 | jpsales@commvault.com