druva

ランサムウェア被害の最小化に向けたインサイダー・ガイド

包括的なデータ保護のための6段階の計画

本ITガイドは、ランサムウェアやその他のマルウェア攻撃による影響を軽減するための実用的な手順を提供します。時間インデックス化されたコピーからデータを迅速に復元することにより、コストがかかり組織を弱体化させる身代金の要求に対処します。

データが人質に

ランサムウェア攻撃は現在流行しているサイバー犯罪であり、影響を受けている組織が世界的に増加しています。ランサムウェアはマルウェア攻撃の一種であり、ほぼすべてのネットワーク侵入手法を悪用した、攻撃者にとって容易でリスクの低い攻撃です。攻撃を受けると、身代金が支払われて復号鍵を入手するまで、組織のデータやコンピュータシステムにアクセスできなくなってしまいます。

ランサムウェアは
1100億円
規模の産業
となる勢いです

CNNの報道によると、2016年第一四半期におけるランサムウェアの被害は2億900万ドル(約230億円) にのぼり、2016年内に10億ドル (約1100億円) 規模になることが予想されています。 FBIはランサムウェアのCryptoWall亜種を使用した攻撃により2015年6月までに1,800万ドル (約20億円) を超える未払い金があると推定しています。さらに2016年第一四半期には昨年全体の4倍の感染率が確認されています。

ランサムウェア攻撃と無縁の業種はなく、特に**ヘルスケア業界**では**特に大きな打撃**を受けてきました。2016年4月に起きた米国メリーランド州のメッドスター・ヘルスという病院グループにおけるランサムウェア攻撃では、10箇所の病院が一週間以上中央ネットワークにアクセスできないまま操業せざるを得ない状態となりました。ハリウッド・プレスビテリアン・メディカル・センターは、2016年2月のランサムウェア攻撃でデータを回復するためにビットコインで1万7,000ドル (約200万円) を支払いました。

あらゆる規模の組織が増加傾向にあるランサムウェア攻撃の被害を受けやすく、リスク低減や攻撃対処に悪戦苦闘しています。

攻撃のオープンドアとなりやすいコンピュータの特徴と実例

コンピュータネットワークをランサムウェアに対してオープンな状態とさせてしまうセキュリティ上の脆弱性は数多く存在します。ほとんどのインシデントでは、疑いを持たない個人が悪意あるリンクや電子メール添付ファイルをクリックしていました。
古いソフトウェアや誤って設定されたソフトウェアもランサムウェアの拡散のために悪用されます。Windowsコンピュータが最大の標的となっていますが、**AndroidやMacデバイスも同様に標的**にされており、安全なコンピュータプラットフォームは存在しないと言えます。Druvaのプロダクトマーケティング担当VPであるデイブ・パッカーは以下のように表現しています。
「結局のところ大きな問題は、何かしらセキュリティホールが存在して、誰かがそれを知っていてそれを悪用しようとしており、その誰かとは常に招かざる人々です。」

従業員にモバイル機器が普及していることも、マルウェア攻撃のリスクを増大させる一因です。多くの企業は組織のファイアウォールで保護されていますが、社員はセキュリティが不十分なモバイルデバイスを使用して企業のデータやサービスに接続しています。同様に、社員や顧客向けにセキュリティ保護されていないモバイルアプリケーションが導入されることにより、新たな攻撃の機会が生まれています。

> “モバイル機器が社員に普及していることもマルウェア攻撃のリスクを増大させています”
>
> – Druva プロダクトマネージメント担当VP デイブ・パッカー

対策を行わなかった場合のコスト

どの組織も幸運を祈りながら自らが標的にされないことを願っていることでしょう。
しかし残念ながら、予防措置を取らない組織に対して深刻な影響を与えるランサムウェアやその他マルウェアによる攻撃が行われる可能性は非常に高いです。被害者は割に合わない身代金を支払うだけでなく、代償を伴う業務停止時間が発生する可能性があります。
また、データ侵害に対する風評被害はもちろんのこと、一部の業界では罰金や罰則を受ける場合もあります。これらすべては非常に高くつきます。実行可能な計画が策定されていない場合、インシデントに受動的に対処していくための時間とお金が必要になります。データを回復するために身代金を支払った企業は、その後も重大なデータ損失の脅威に直面します。
ファイルが復号処理中に変更されてしまった場合、特に訴訟中である組織では、データ改ざんによるリスクがもたらされます。さらにランサムウェアの被害者の多くは、身代金を支払ったにも関わらずデータを復旧できなかったことを忘れないで下さい。

予防手法は有用だが限定的

データの境界を保護することは、ランサムウェアやその他のマルウェア攻撃を回避するアプローチの一つです。定期的なセキュリティ、アンチウイルスやアンチマルウェアソフトウェア、オペレーティングシステムのアップデートのように、エンドユーザーの意識とスマートブラウジングの実践が重要です。攻撃者は十分に保護されていないデータを搾取するため、組織は時代遅れのITインフラを移行していく必要があります。

修正プログラムは確かに攻撃を防止する役割を果たしていますが、限定的であり、保護レベルが不十分で変わりやすくなります。データ保護スキームをどう変更するにせよ、マルウェア攻撃は巧妙化され、攻撃者は新しい侵入方法を見つけてきます。このことは、現在のマルウェア対策ベンダーは

いたちごっこを繰り返しており、重箱の隅には常に脆弱性が存在していることを意味します。誰かがその脆弱性を見つけ、それを悪用するのは時間の問題です。言い換えると、多くの組織にとってランサムウェア攻撃はますます避けることのできない問題になっています。

これまで以上に危険性が高まり検出が難しくなるランサムウェア攻撃を防御するうえでもう一つの弱点となるのが、多忙かつモバイル化する従業員のコンプライアンス遵守に依存するユーザーの意識です。いくつかの保護策が提供される一方、ユーザーが自分のコンピューティングデバイス上にウイルスやマルウェアを誤ってダウンロードしてしまった場合、暗号化は役に立ちません。さらにランサムウェアは多くの場合、ネットワーク経由で拡散した後に休止状態を続けるよう設計されており、発信元を特定しにくくしています。マルウェア防御手法では保護が不十分であることを考えると、組織がそれだけに依存するのは危険です。

データのバックアップでランサムウェアを阻止し、他の利点も享受

ランサムウェアや他のマルウェアのインシデントに対する最善の防御策は、包括的なデータ保護計画であることを専門家は同意しています。具体的には、サーバー、PC、クラウドアプリを横断した自動化および時間インデックス化されたバックアップデータのスナップショットによって、情報を元の状態に復元させることが可能です。その結果、組織は攻撃前の任意の時点のデータにアクセスできるようになります。

攻撃に直面したとき、確固としたバックアップ計画がどのように組織のセキュリティを向上させ、交渉の立場を優位にするかを確かめるのは簡単です。エンタープライズグレードのデータバックアップでは、データ損失がマルウェアやシステム障害、人的エラーのどれによるかを問わず、ランサムウェアとは関係のないさまざまな利点も提供されます。正しいデータバックアップソリューションは優れた情報ガバナンスを促進し、組織による監査証跡の閲覧やコンプライアンス目的のためのデータ保護が行える機能を提供します。クラウドベースのバックアップソリューションでは、オンプレミスのデータが危険にさらされたときに緊急のオフサイトストレージが提供されます。

データバックアップの6段階の計画

Druvaのデータ保護専門家が記した、IT部門がデータを安全に保つために利用できる6段階の能動的な手順を概説します。これら手順は非常に効率的にシームレスに実行され、エンドユーザーに負担をかけないバックアップ計画の基盤となります。

1. **分散データの保護: “どのように”**
   デバイス、デスクトップ、Office 365のようなクラウドアプリを横断して定期的にバックアップを行うエンタープライズグレードの自動バックアップソリューションは分散データを保護し、ランサムウェア被害に遭った場合、またはその他の侵入が発生した場合に保険としての役割を果たします。必ずオフサイトストレージを提供するクラウドベースのバックアップソリューションを選択するようにしてください。
   オフサイトストレージはAWSやAzureのストレージロケーションを活用し、オフサイト機能を提供するだけでなく、現地のストレージリージョンに保存することでローカルのデータレジデンシー法にも準拠します。

2. **分散データのバックアップ: “誰を”**
   現在のバックアップ計画は地理的に分散した部門を含めて100%のユーザーを対象にしていますか？潜在的なデータ損失リスクを低減するために、保護を必要とするすべてのエンドユーザーを対象に、自動的に展開するバックアップ計画の適用範囲を確認し、検証してください。少なくとも主要なユーザーがデータ保護ポリシーの対象となっていることを確認する必要があります。

3. **データバックアップ範囲の検証: “何を”**
   何をバックアップ対象としていますか？おそらくデスクトップ上や電子メールは保護しているでしょう。しかしプロファイル、システムとアプリの設定、フォルダなど他のユーザー固有データはどうでしょうか？保護されたユーザーのすべての重要データがバックップされるよう、バックアップ対象を確認および検証し、必要に応じて変更することが強く推奨されます。より包括的な計画が必要な場合、カスタムフォルダの作成を検討してください。ユーザーがバックアップ用のデータをカスタムフォルダに保存することで、将来的なデータ損失を削減します。

4. **分散した部門ごとにバックアップ頻度を確認: “いつ”**
   どのくらいの頻度でバックアップを行っていますか？2日か、8時間か、4時間でしょうか？役員や幹部向けにさらに短い間隔が必要でしょうか？保護されたすべてのユーザーに対してミッションクリティカルなデータを自動で定期的にバックアップを行えるようにするため、バックアップ頻度を確認および検証し、必要に応じて変更します。一般的な目安として、最低でも4時間ごと、主要ユーザー向けには2時間ごとにデータをバックップすることが推奨されます。また、特定のユーザーや部門の要求に応じて別々のバックアップ頻度を選択することもできます。

5. **保存ポリシーの検証: “どの期間”**
   バックアップデータをどの期間保持しますか？14日か、7週間か、6か月でしょうか？社内目標を満たし、特に重要なユーザーや部署のために十分なRPO (Recovery Point Objective; 目標復旧時点) を達成するよう確認および検証し、必要に応じて長期間の保存ポリシーを採用してください。データ保存ポリシーは業界や規制、社内のITポリシーによって異なります。IT部門、法務部門、コンプライアンスチームでデータ保持期間の要件を検討する必要があります。

6. **定期的なポリシーの見直し: “将来への準備”**
   上記対策により当面の間は十分な保護が行えるでしょうが、組織のニーズを満たすよう、おおむね半年ごとにバックアップポリシーを見直すことが強く推奨されます。この定期作業は主にIT部門が担いますが、場合によっては法務部門と連携して作業するようにします。

Druva inSyncで行えること

業界No.1と評価された企業向けエンドユーザーデータ保護ソリューションであるDruva inSyncを使用し、被害に遭う前に完全なバックアップを実施することで、IT部門はランサムウェア攻撃からの復旧に役立てることができます。Druva inSyncはラップトップ、デスクトップ、スマートフォン、タブレットなどのエンドポイントとクラウドアプリケーション向けに設計され、自動化されたエンタープライズグレードのバックアップソリューションを提供します。ネットワークやユーザーが攻撃を受けた場合、ハードウェアが永久にロックされたとしても、迅速にデータを復元できるようになります。inSyncは具体的には以下の機能を提供します。

時間インデックス化された自動バックアップ: inSyncはユーザーデータおよびユーザー固有のシステムとアプリ設定を時間インデックス化されたスナップショットを使用したバックアップを提供します。これによりデータを簡単に攻撃前の元の状態に復元することができます。

即時データアクセス: inSyncを使用すると、組織はどこからでもデータへ即時アクセスできるようになり、ユーザーがランサムウェアやその他のマルウェアによる影響を受けなくなります。

高頻度のバックアップ: inSyncを使うと組織は最短5分間隔でデータをバックアップできるようになります。

マルチゾーンの冗長化: 各データセンターはビジネス継続性を確保するためマルチゾーンで冗長化され、最高レベルのデータ信頼性と保証された可用性が提供されます。

多彩なストレージオプション: データストレージやプライバシー、セキュリティのニーズに最も適合するよう、inSyncは世界規模のストレージオプションとして多くの選択肢（AWSまたはMicrosoft Azure）を顧客に提供し、希望するインフラベンダーを選択できます。

モバイルデバイスの適用範囲: ファイアウォール外部のモバイルデバイスはマルウェアに感染させるための標的となります。エンドポイント上のデータバックアップは不可欠であり、inSyncではエンドポイント上のデータもバックアップ対象となります。

使いやすさ: inSyncは不安定なネットワーク上でもユーザーに影響を与えず、バックアップや復元を確実に行うために最適化されています。

ユーザーによるフォルダ追加: すべての重要データが保護されるようにするため、inSyncではエンドユーザーによるフォルダ追加が行え、バックアップ対象のデータをユーザー自身で選択することができます。エンドユーザーは個人情報やアプリケーション設定とともに自身のデータを自己復元することもできます。

まとめ

本ITガイドで概説される手順に従い、エンタープライズソリューションとしてDruva inSyncを選択することでIT部門はランサムウェアやその他のマルウェア攻撃の影響を軽減する強固なバックアップ基盤を実装することができます。時間インデックス化されたコピーから迅速にデータを復元する機能を持つことで、コストがかかり組織を弱体化させる身代金の要求に対処します。業界をリードするクラウドバックアップがあれば、暗いニュースを気にする必要はありません。

Druvaはモバイルワーカーにデータセンターレベルの可用性と内部統制を実現する統合型データ保護のリーダーです。バックアップ、可用性、内部統制を単一のダッシュボードで提供するDruvaの受賞歴あるソリューションはネットワークへの影響を最小化し、ユーザーに対して透過的です。業界で最も急速に成長しているデータ保護プロバイダとして、Druvaは4000社以上のグローバル企業で400万以上のデバイスにて利用されています。詳細はjp.druva.com を参照してください。

Q117-CON-10587

Druva合同会社
japan-sales@druva.com
jp.druva.com