悪意あるランサムウェアの脅威からデータを保護する

このデータのアベイラビリティのベスト・プラクティスは、あらゆる企業がランサムウェア攻撃による潜在的なデータ消失やダウン時間に対して効率的に準備をし、それらを回避できるように設計されています。業界のベスト・プラクティスに従うことによって、ITマネージャーは身代金の支払いを回避でき、HPEとVeeam®ソフトウェアを利用して日常的な運用のための堅固なデータ・アベイラビリティ・ソリューションを作成できます。

「個人や組織をランサムウェア攻撃から完全に守る方法やツールはありません。しかし、ビジネスの復元と継続性にとっては、非常事態計画や改善計画がきわめて重要です。そして、これらの計画は定期的にテストしなければなりません。」

– 前FBIサイバー部門アシスタント・ディレクター、James Trainor氏。

この引用からユーザーが理解できるのは、ランサムウェアは最終的にネットワークに侵入する脅威の一部に過ぎないということです。最適なソリューションは、ユーザーのデータを保護することです。**fbi.gov/news/stories/incidents-of-ransomware-on-the-rise**

ランサムウェア攻撃の増加

ランサムウェア攻撃は、規制およびコンプライアンス要件、脆弱なネットワーク、そして不十分なバックアップ・ベスト・プラクティスに付け込むことによって、複数の業種に拡大し続けています。脅威が拡大するにつれ、あらゆる範囲の業種や企業がますます多く標的となり、利用されることになります。たとえ強力なサイバー・セキュリティのソリューションやプラクティスを用いたとしても、ネットワークには絶えず侵入が繰り返されています。Institute for Critical Infrastructure Technology (ICIT) によると、2016年と2017年はランサムウェアが企業に打撃を与える年になると予測されています。ランサムウェアの脅威は、「企業のほぼ40%が攻撃を受けて」増加傾向にあります。[1]

ランサムウェアによる企業およびIT部門のリスク

ランサムウェア攻撃は、単なるセキュリティのリスクにとどまりません。ランサムウェアの被害にあった企業は、財政上および技術上の問題と同時に、取り返しがつかないほどのブランド力の低下に直面します。

財政上の破綻

身代金のコスト、ITにかける貴重な時間の消失、そしてミッションクリティカル・アプリケーションへの潜在的なダウン時間により、企業は回復不能な被害を受ける可能性があります。

IT部門への打撃

ハッカーは、将来の攻撃の可能性に備えて、被害者のネットワークへの制御とアクセスを保持しています。ITマネージャーは、繰り返し発生する脅威に直面することで、より多くのリソースをランサムウェアの阻止に費やし、ビジネスにとって不可欠な重要なITプラクティスから時間を吸い上げることになります。

企業ブランドへのダメージ

多くの場合、評判の失墜、顧客の喪失、市場占有率の低下を避けるため、企業はランサムウェア攻撃について報告しません。しかし、身代金を支払ったり、データのバックアップをしなかったりする企業は、最終的にはブランド・アイデンティティや市場での評判への深刻なダメージを引き起こす、より注目を集める攻撃の被害者となります。

成功例—Veeamの使用によるランサムウェアからの防御の成功

イングランドのBedford Schoolは、CryptoLockerウィルスによる悪意あるランサムウェア攻撃の被害を受け、教職員のコンピュータが感染し、すべてのファイルが暗号化されました。この学校には高額の身代金を支払うための資金がなく、ネットワークのダウン時間を追加できる余裕もありませんでした。

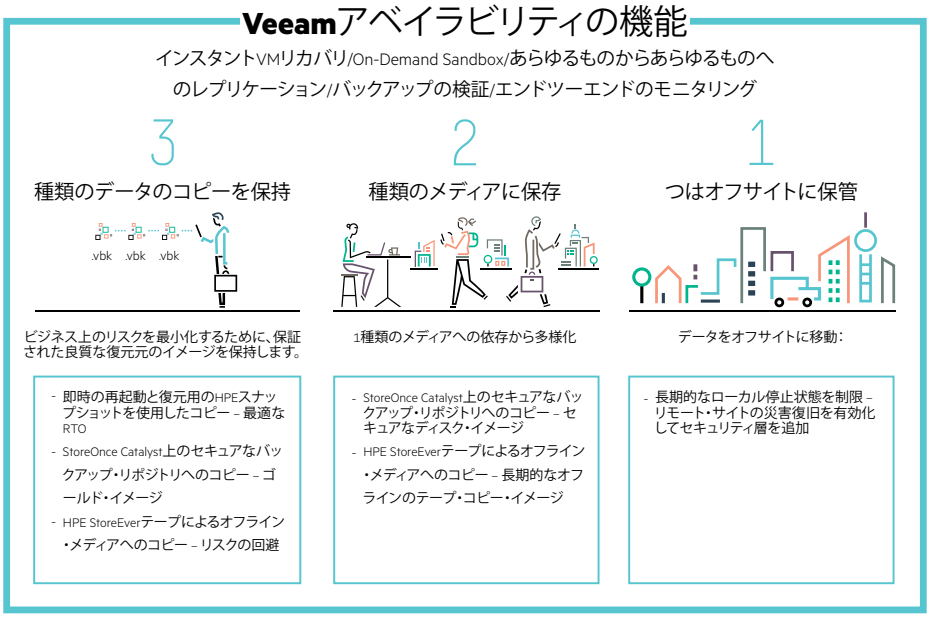
BedfordのITチームは、3-2-1バックアップ・ルールに従うことで、身代金をまったく支払わずに済み、ネットワーク機能を失うこともありませんでした。Veeamは、暗号化されたファイルをすべて迅速に復元する支援を行いました。

[1] 「**ランサムウェアの脅威は、「企業のほぼ40%が攻撃を受けて」増加傾向にあります**。」2016年8月、The Guardian。

VeeamとHPEによるソリューションの概要
VeeamとHPEの業界をリードするソリューションは、あらゆる規模の企業が悪意のある攻撃と闘い、データを保護できるように完全に対応しています。

- **迅速なデータのリストアとリカバリ**
  HPEストレージ・スナップショットを使用すると、高速の仮想マシン(VM)と段階的なリカバリによって、暗号化されたランサムウェアのデータベース、アプリケーション、ファイル、およびオペレーティング・システム(OS)をオーバーライドできます。HPE 3PAR StoreServ、Store Virtual、StoreOnce、およびStoreOnce Catalystとの実証済みの統合により、迅速に復元し、アプリケーションのダウン時間を回避します。
- **インフラストラクチャのロックダウン**
  ランサムウェアは、ランサムウェアが確認できないもの感染させることはできません。HPEは、StoreOnce Catalystとの統合によってこれを実現します。この統合により、バックアップ・イメージをランサムウェアに対して非表示にし、リストアを可能にします。オフライン・テープおよび非同期リモート・レプリケーション・コピーを通じて、付加的な保護レイヤーが追加されます。
- **テスト環境**
  Veeam On-Demand Sandbox™およびVeeam SureBackupを用いてVMを本番環境にリストアする前に、ランサムウェア・アイテムを迅速にテストして削除します。
- **組み込まれた使いやすさ**
  Veeam ONE™モニタリング、レポート作成、およびキャパシティ・プランニング・ツールにより、内蔵のバックアップ評価を利用して、重要なVMが確実に保護されるようにします。

これらの機能は、Veeam Availability Suite™およびHPEストレージとの統合では標準装備です。このソリューションには特別なスクリプトは必要なく、HPEとVeeamの標準の製品を利用します。



HPEとVeeamによるランサムウェア・ソリューション

VeeamとHPEによるこのデータ・アベイラビリティ・ソリューションは、ハッカーによるあらゆるランサムウェア攻撃と闘うために設計されています。Veeamの3-2-1バックアップ・ベスト・プラクティスに従うことで、企業はデータの整合性とアベイラビリティを確保できます。上記の図は、業界をリードする推奨事項に沿った3-2-1ルールを表したものです。

ランサムウェアに3-2-1バックアップ・ルールを利用する

3-2-1ルールの目標は、アプリケーションの稼働時間とデータのアベイラビリティを最大化するデータ保護ソリューションを顧客に提供することです。3-2-1バックアップのベスト・プラクティスを正しく実行することで、ITマネージャーは次に挙げる弊社の3-2-1ガイドラインに従ってデータを保護できます。

- データの3つのコピーを保持し(プライマリ・データと2つのコピー)、不具合のあるバックアップでデータを消失しないようにする。
- バックアップのコピーを、異なる2つのタイプのメディア(テープ、ディスク、セカンダリ・ストレージ、クラウドなど)に保存する。
- 内部に問題が発生した場合やランサムウェアによるネットワーク内の感染の場合に備え、1つのコピーをオフサイトで(テープまたはクラウドのどちらか)保管する。

サマリー

データのアベイラビリティ・ソリューションは、既存の技術から成る完全に統合されたソリューションです。このソリューションは、組織をランサムウェア攻撃から迅速に復旧させるだけでなく、エンタープライズ・クラスのデータ・アベイラビリティ・ソリューションも提供します。この柔軟で手頃なベスト・プラクティス・ソリューションは、Veeamの認定パートナーによってすぐに実装できます。

Veeam Backup & Replication™を用いて3-2-1ルールに従う方法のブログの詳細はこちら。

a00000445jpn、2017年1月