COHESITY

ヒントシート

ランサムウェアがバックアップを攻撃する5つの手法…そしてそれを防止する方法

概要

バックアップとリカバリソリューションは組織を保護するためのものですが、Locky や Crypto などの高度なマルウェアは、バックアップデータをターゲットに攻撃を仕掛けるようになってきています。ランサムウェア攻撃が頻発し、拡大していることを考えれば当然の流れといえるでしょう。最初にランサムウェアに身代金が支払われたのは、1989 年前後のことでした。これが発端となり、ハッカーが無防備なターゲットのデータをロックし、所有者が身代金を支払うまでロックを解除しないという手口の攻撃がいたるところで発生するようになりました。Cybersecurity Ventures の調査によると、2019 年、企業は 14 秒に 1 度の頻度でランサムウェア攻撃を受けました。このような理由から、以下の 5 つの検討事項を念頭に置き、バックアップを狙ったランサムウェア攻撃をうまく防御して、検出し、すばやい対応をとるための戦略を練ることが重要になってきます。

1. 高度なランサムウェア攻撃は、バックアップという保険を負債に変える

サイバー犯罪者は、シャドーコピーであるバックアップデータを積極的に攻撃するようになっており、事業継続のための保険と見なされてきたバックアップを完全に支配し、さらにひどい場合には、破壊しようとしています。その攻撃は高度化しており、エンドポイントからプライマリ環境に侵入すると真っすぐバックアップ(現在、企業データの80%が保管されています)へと向かい、そこにあるすべてデータを削除するか侵害するかしたうえで、本番環境を乗っ取ります。バックアップを狙ったランサムウェア攻撃を防ぐには、多層的な防御が必要です。オリジナルのバックアップデータはイミュータブルな(変更不可の)状態で保存されるべきであり、データのゴールドコピーは外部システムからマウントされないようにする必要があります。また、多要素認証(MFA)とスナップショットのWORM(Write Once Read Many)もなくてはならない機能です。

2. 攻撃対象が拡大により、バックアップがランサムウェアの攻撃対象に

データの爆発的な増加 (IDCの推測によると、2025 年には世界に存在するデータの量は175ゼタバイトを超えると見られています) と大量データの断片化――バックアップのために複数の単一機能製品 (メディアサーバー、マスターサーバー、ターゲットストレージ、その他) に依存し、いくつもの異なるサイロに分散していること――により、組織の攻撃対象が拡大しています。その結果、バックアップデータはサイバー犯罪者にとってアクセスしやすいものとなっています。ランサムウェアを未然に防ぐには、まず何よりも企業の攻撃対象を減らし、どこにどのようなデータが置かれているのかを把握しておくことが必要です。インフラストラクチャー、ワークロード、バックアップロケーションをつなぐ統合ソリューションにより、大量データの断片化を解消することで、ランサムウェア攻撃から組織を守ることができます。

数字で見るランサムウェア

- 14秒に1件の頻度でランサムウェア攻撃が発生
- 2016年から700%増加
- 攻撃者の35%が身代金の獲得に成功
- 金銭、生産性、ダウンタイムで110億ドル相当の損失

"

ランサムウェアの作成者はバックアップが有効な防御であることを認識しており、バックアップを見つけ出し、排除するようマルウェアを改変している。

CSO Magazine

3. 断続的な監視はバックアップへの攻撃を容易に

サイバー攻撃は、外部からだけでなく、内部からも仕掛けられることがあります。例えば、不満を持った従業員が、大量のデータを変更または削除しようとするケースも考えられます。このような行動を検出するために、バックアップデータの取り込みの変化率だけに頼っていたのでは不十分で、攻撃をリアルタイムに検出することが必要です。必要なのは、ファイルと監査ログを分析し、例え注意を払っていない時でも、わずかな変化率を継続的に監視し、検出することができるソリューションです。適切なバックアップソリューションは、一瞬たりとも休むことなく、サイバー攻撃から組織を守ってくれます。

4. クリーンリストアのための可視性の欠如

ランサムウェア攻撃後のリストアはストレスの多い作業であり、一刻を争います。バックアップスナップショットの可視性がなく、誤って改ざんされたスナップショットをリストアしてしまい、ソフトウェアの脆弱性とサイバー脅威をITの本番環境に再度取り込んでしまったとしたらどうなるでしょう。リカバリは迅速に行う必要がありますが、クリーンなリストをを行うことも必要です。バックアップソリューションには、スナップショットの健全性とリカバリ性を深く可視化し、クリーンなリストアポイントを提示することが求められます。

5. バックアップとリカバリに時間がかかることでランサムウェアの被害が深刻化

合成フルバックアップが必要なレガシーバックアップを利用していてランサムウェア攻撃の被害にあった場合、ITチームによるリカバリに数日を(場合によっては数週間も!)要することが考えられます。Ponemon Instituteの最新のレポートによると、1回のランサムウェア攻撃の平均コストは500万ドルであり、その主な原因として、生産性の低下、システムのダウンタイム、情報の盗難があげられます。ランサムウェア攻撃にすばやく対応し、パブリッククラウドを含むグローバルなデータフットプリント全体で感染したファイルをただちに見つけて削除することができるバックアップとリカバリソリューションが必要です。また、数百台の仮想マシンを、任意の時点にすばやく大規模にリストアできるインスタントマスリストア機能もあわせて必要になってきます。

ランサムウェア攻撃の防止、検出、迅速な復旧

多くの組織がサイバー攻撃による損失をゼロに抑え、ランサムウェアの支払い要求を自信をもって拒否したいと考えています。ランサムウェアの攻撃を防ぎ、検知し、迅速に復旧させるには包括的なアプローチでデータを保護する必要があります。

データ防御について詳しく解説したeブックはこちらからダウンロードいただけます。

COHESITY