COHESITY

ヒントシート

ランサムウェアがバックアップを無力化する5つの手法

概要

バックアップとリカバリのソリューションは企業を保護する必要がありますが、LockyやCryptoのような巧妙なマルウェアはバックアップデータも狙うようになりました。今日のランサムウェア攻撃は、より頻繁かつ広範囲に及んでおり、データをロックして身代金を支払うまで保持するだけではなく、データを守るために設計されたシステムそのものを危険にさらすという、より精密なものになっています。Cybersecurity Venturess社によると、ランサムウェアは2021年末までに11秒に1回のペースで企業を攻撃するようになりました。そのため、バックアップデータを保護する最善の方法について戦略を練る際には、次の5つの留意点を検討し、もし最悪の事態が発生した場合には、ランサムウェアの攻撃に迅速に対応できるようにしておくことが重要です。

1. 巧妙なランサムウェア攻撃は、保険であるはずのバックアップをマイナスにする

サイバー犯罪者は現在、バックアップデータを積極的に狙い、長い間、事業継続のための保険と考えられてきたバックアップを完全に制御したり、あるいは最悪、破壊したりしてきます。より巧妙化した攻撃は、エンドポイントからプライマリ環境に侵入し、企業データの80%が保存されているバックアップに直接向かい、本番環境を乗っ取る前にすべてを削除するか、破壊します。ランサムウェアによるバックアップへの攻撃を防ぐために必要なのは、多層的な防御です。オリジナルのバックアップデータはイミュータブルな (変更不可能な) 状態で保管し、そのデータのゴールドコピーに外部システムから絶対マウントしてはいけません。バックアップソリューションの一部として、WORM (Write Once Read Many: 追記型)、データ暗号化、ビルトイン耐障害性、最新のデータ分離などのルールは、ランサムウェア攻撃に対して追加の保護レイヤーを提供します。

2. 攻撃対象の拡大により、バックアップがランサムウェアの攻撃対象になる

IDCの報告によると、2020年に64.2ゼタバイトのデータが作成または複製され、2025年にはそのデータ量は175ゼタバイト以上になると推測しています。増大するデータを保護するために、企業はこれまでバックアップのために複数のポイント製品 (メディアやマスターサーバー、ターゲットストレージなど) に依存し、これらの製品は、オンプレミスやマルチクラウドにまたがる広大なサイロを形成するため、組織の攻撃対象領域を拡大し、サイバー犯罪者がバックアップデータにアクセスしやすくなる状況を作ってきました。ランサムウェアの侵入を防ぐには、どのようなデータがどこにあるのかを把握することも含め、まず企業の攻撃対象領域を減らし、大量データの断片化という問題に対処する必要があります。インフラストラクチャ、ワークロード、バックアップロケーションの可視性を高める統合ソリューションは、ランサムウェアからデータをより強固に保護します。

数字で見るランサムウェア

- 11秒に1回、ランサムウェア攻撃が発生[1]
- 2025年までに全世界で10.5兆ドルの被害が発生[1]
- 2020年7月から2021年6月の間に前年比1,070%増加[2]
- 金銭的被害は、実際の身代金要求額の10倍から15倍に[3]

> ランサムウェアの作成者は、バックアップが有効な防御手段であることを認識しており、バックアップを追跡して削除するようマルウェアを改変している。
>
> **CSO Magazine**

[1] Cybersecurity Ventures
[2] Fortinet 2021 Ransomware Survey Report
[3] Gartner: How to Prepare for Ransomware Attacks, November 2020

3. ユーザー認証情報の漏洩は、ランサムウェアへの継続的なギフトとなる

盗まれた認証情報は、バックアップを含むIT環境のさまざまな部分へ絶え間なくアクセスすることを可能にし、サイバー犯罪者がより大きな利益を得るためにデータを流出させることもできるため、ランサムウェア攻撃者にとって聖杯のような存在となっています。 2021年Verizon Data Breach Investigationsレポートによると、意図的なデータ侵害における一般的なデータの種類は認証情報の漏洩で、61%という驚異的な数の侵害に関与しています。ロールベースのアクセス制御 (RBAC)、多要素認証 (MFA)、継続的な監視機能など、ユーザーアクセスを厳しく管理することができるモダンバックアップを導入することで、企業はランサムウェア攻撃への対策がより効果的に行え、ダウンタイムや生産性への悪影響も防ぐことができます。

4. 可視性と早期発見の欠如は、攻撃者を有利にする

ランサムウェアの攻撃者は、ダークデータの中で繁栄しています。彼らはバックアップをロックし、本番システムへ移動して密かにデータを削除し、ダークウェブでデータを売ることができます。信頼性の高いバックアップと次世代データ管理ソリューションを使用した早期発見は、悪質な攻撃者の動きを鈍らせる良いきっかけとなりますが、ランサムウェアの流出攻撃を発見するには、人工知能と機械学習 (AI/ML) を活用したほぼリアルタイムの検知が必要となります。アラートを含む自動化されたインテリジェンスは、より迅速な攻撃発見を可能にしながらも、ITスタッフは夜間や週末をゆっくり過ごすことができます。

5. 長い復旧サイクルがランサムウェアの被害を拡大させる

ランサムウェアの被害に遭った企業が、合成フルバックアップを必要とするレガシー製品を使用している場合、そのITチームは復旧に数日 (もしくは数週間) を費やすことになります。最近のPonemon Instituteのレポートによると、1回のランサムウェア攻撃による平均コストは、主に生産性の低下、システムのダウンタイム、情報の窃盗によって500万ドル (約5億円) に上るとされています。必要なのは、ランサムウェアの攻撃に迅速に対応し、パブリッククラウドなどのグローバルなデータ基盤からデータのクリーンコピーを迅速に探し出すことができるバックアップとリカバリのソリューションです。また、何百台もの仮想マシン (VM)、データベース、大量の非構造化データを任意の時点に即座に復旧できる、即時の大量復旧機能も必要です。

ランサムウェアによるサイバーデータ流出を阻止し、データを守る

サイバーリスクを軽減し、身代金の支払い要求を拒否する自信を持ちたいなら、バックアップとデータ管理ソリューションがサイバーレジリエントであることを確認する必要があります。ランサムウェアの攻撃から身を守るには、バックアップが標的にならないように守り、完全な可視化と早期検知で侵入を阻止し、迅速かつクリーンな大規模復旧でダウンタイムとデータ損失を低減する包括的なアプローチしかありません。

データの防御についてさらに詳しく知るにはこちらからeBookをダウンロードしてください。

COHESITY

Cohesity.com/jp | Cohesity Japan 株式会社 | 東京都千代田区大手町1-6-1 大手町ビル4F

9100003-006-JP 2-2022