DELL Technologies

バックアップ侵入 ：デル・テクノロジーズでサイバーセキュリティとレジリエンスを強化

概要

バックアップ侵入は、重要な情報を保護するよう設計されているシステムの脆弱性を悪用します。これにより、あらゆるセクターの企業に対する脅威が増大しています。この攻撃はデータ リカバリー システムを侵害し、信頼を低下させ、業務を危険にさらします。重大な経済的損失、ダウンタイムの延長や評判の低下など、深刻な影響をもたらす可能性があります。

デル・テクノロジーズは、機密データを保護し、このような攻撃を防ぐためのエンドツーエンドの防御スイートを提供しています。これには、Dell Trusted Device、Dell Trusted Infrastructure、そしてすべてのソリューションに統合された広範なセキュリティ機能などがあります。Dell は、戦略的パートナーシップとプロフェッショナル サービスを追加することで、組織がレジリエントな多層型セキュリティ フレームワークを確立し、バックアップ侵入インシデントを効率的に検出して阻止し、このようなインシデントから復旧できるよう支援します。

Dellの革新的なソリューションと専門家によるサポートを導入することで、企業はインフラストラクチャを保護し、事業の継続性を維持するための準備を強化できます。

バックアップ侵入の脅威の増大

バックアップ システムは事業の継続に不可欠で、ランサムウェアやハードウェア障害などのサイバー イベント後のリカバリーに貢献します。残念ながら、このまさに命綱といえる存在そのものがサイバー犯罪者の標的となっています。バックアップ侵入によってバックアップ データが破損されたり、削除されたりして、最も必要なときにデータにアクセスできなくなります。

このような進化する脅威に対処するには、プロアクティブな対策が必要です。バックアップ システムを適切に保護できなければ、運用が危険にさらされ、機密データが漏洩します。小規模企業から多国籍企業まで、あらゆる規模の企業が攻撃対象となる可能性がありますが、特に医療、金融、製造などの業界がリスクにさらされています。

デル・テクノロジーズは、バックアップ環境を強化する緊急性を認識しており、高度な攻撃に対処するための高度なツールとガイダンスを提供しています。

バックアップ侵入攻撃

バックアップ侵入とは、サイバー犯罪者がバックアップ システムの脆弱性を悪用して、重要なリカバリー データを侵害、破壊、暗号化することです。この高度な攻撃は、他のインシデント（ランサムウェアやマルウェアの導入など）と同時に行われるか、またはその後に行われる可能性があり、運用面と財務面での影響が深刻化します。

バックアップ攻撃の手法

1. **初期の侵害：**攻撃者は多くの場合、フィッシング、脆弱な認証情報、パッチが適用されていない脆弱性を介してネットワークに不正アクセスします。
2. **ラテラル ムーブメント：**ネットワーク内に侵入すると、攻撃者はツールを使用して検出されないまま移動し、バックアップ リポジトリーと重要なデータセットを狙います。
3. **バックアップの侵害：**主な手口には、バックアップ ファイルの暗号化、リカバリー ポイントの削除、データの破損などがあります。

一般的な手法

- **認証情報の盗難**バックアップ システムにフルアクセスできる管理者アカウントが侵害されます。
- **ランサムウェアの展開**ライブ データとバックアップの両方が暗号化され、復号化のために金銭の支払いが要求されます。
- **時限式破壊**検出を回避するため、バックアップを徐々に侵害します。リカバリーが必要な時に企業が危険にさらされることになります。

このような技術は、脅威の高度さと深刻さを浮き彫りにしており、事前の対策が求められています。

ビジネスへの影響

経済的損失

バックアップ侵入により、リカバリー コストとダウンタイムが増大します。通常、対応コストは2倍または3倍になります。暗号化されたバックアップや侵害されたバックアップからのリカバリーには、攻撃者への支払い、新しいインフラストラクチャの構築、高額なコンサルタントの利用が必要になる場合があります。

業務の中断

実行可能なバックアップがないと、リカバリー時間が長くなり、これによってサービスの中断、プロジェクトの遅延、重要な機能の停止が発生します。

評判への影響

データが永久的に失われる場合や、ダウンタイムが長引く場合には、ステークホルダーの信頼を損ない、ビジネスの長期的な実行可能性が損なわれる可能性があります。

実例

あるグローバルな医療機関では、ランサムウェア攻撃中にバックアップが破損していることが判明しました。身代金を支払ったにもかかわらず、3週間分の患者データが完全に失われ、手術に遅延が生じて訴訟につながりました。リカバリー コストは総額**5,000万ドル**を超えました。

警戒すべき統計

最近の調査によると、バックアップ システムの侵害による平均的な経済的被害は、罰金、ダウンタイム、リカバリー費用を含めて**445万ドル**[1]を超えると推定されています。特に憂慮されるのは、このようなインシデントの発生頻度が増加していることです。グローバル レポートによれば、バックアップ関連の脅威は前年比で**39%**増加しています。

57%
バックアップを狙った攻撃でのバックアップ リポジトリーへの侵入成功率

出典：Index Engines（2024年）

デル・テクノロジーズでバックアップ侵入に対処

デル・テクノロジーズは、バックアップ侵入攻撃がもたらす特有の課題に対処するための堅牢なツールとサービス スイートを提供し、企業が効果的に防止、検出、復旧できるようにします。

サーバーおよびストレージ セキュリティ ソリューション

Dellのサーバーおよびストレージ ソリューションは、バックアップを狙う攻撃に対する比類のないレジリエンスを提供します。組み込みの機能によりバックアップの安全性を確保し、スナップショットが侵害されないようにします。

- **不変バックアップ/スナップショット：**改ざん防止リストア ポイントを作成します。
- **エアギャップ型リカバリー：**データをライブ ネットワークから分離して破損を防止します。

[1] Ponemon、『Cost of a Data Breach Report 2024』

Dell Data Protectionアプライアンスを強化

Dell Data Protectionアプライアンスには、ファームウェアの整合性を確保するDell SafeBIOSや、安全な暗号化でバックアップ攻撃を防御するSafeDataなどの機能が組み込まれています。さらにこれらのソリューションは、多要素認証(MFA)、ロールベースのアクセス制御(RBAC)、デュアル認証などの機能を備えており、脅威アクターによる侵入を防止します。

CrowdStrikeによる高度な脅威検出

CrowdStrikeとDell Data Protectionの連携では、一連の高度な機能を通じてデータ保護環境のセキュリティとモニタリングを強化することに重点を置いています。

1. **エンドポイントとデータの保護：**Dellは、CrowdStrikeのエンドポイント セキュリティと拡張検出および対応(EDR/XDR)をデータ保護ソリューションに統合しています。これには、DellのPowerProtect Data ManagerとPowerProtect Data Domainからのテレメトリー収集と、CrowdStrike Falconコンソールと次世代SIEMソフトウェアからのセキュリティ インサイトなどがあります。
2. **モニタリングと対応：**DellのManaged Detection and Response (MDR)サービスは、お客様に代わってCrowdStrikeソフトウェアを管理し、ログを収集して、侵害の兆候(IoC)や異常検出を調査します。この統合により、Dellは継続的なモニタリング機能を提供し、お客様のSOCと協力して、脅威を迅速かつ効果的に修復できます。
3. **リアルタイムでの可視化とデータ移動制御：**CrowdStrike Falcon Data Protectionプラットフォームは、さまざまなソースとチャネル間のデータ移動をリアルタイムで可視化し、コンテンツとコンテキストの両方でデータを分類します。これにより、コンテンツとコンテキスト分析を組み合わせて、データの盗難を防止し、データ保護ポリシーを効果的に適用することができます。
4. **一元化された管理とシンプルな導入：**この統合により、1つのプラットフォームとエージェントでエンドポイントとデータの両方の保護を管理できるため、複雑さと運用オーバーヘッドが軽減されます。これは、CrowdStrike Falconプラットフォームの軽量でクラウドネイティブなアプローチにより促進されます。これにより迅速な導入が可能になり、また中断を最小限に抑えることができます。

CrowdStrikeとDell Data Protectionの統合では、高度なEDR/XDR機能、リアルタイム モニタリング、包括的なデータ管理を活用して、データ保護環境の全体的なセキュリティとレジリエンスが強化されます。

最近PowerProtect Cyber Recoveryを導入したある大手金融機関では、侵害発生時に攻撃者が重要なバックアップの90%にアクセスできないようにしました。その結果、身代金を支払うことなくシームレスに復元できました。

Dell PowerProtectソリューションでバックアップの整合性を実現

Dell PowerProtectは、不変性、分離、圧縮を活用してバックアップ システムの侵害を防止する包括的なバックアップ保護を提供します。PowerProtectとランサムウェア検出ツールが統合したことで、不審な変更が発生するとアラートがトリガーされ、即座に対処できるようになります。

多層型セキュリティ アプローチ

データを保護するには、調整された多面的なセキュリティ戦略が必要です。Dellは、レジリエンスに優れたバックアップ環境を構築するための業界ベスト プラクティスを企業が導入できるよう支援します。

防御を強化するための重要なステップ

- **ゼロトラスト原則の採用：**すべてのユーザー、デバイス、プロセスを継続的に検証し、不正アクセスのリスクを軽減します。
- **すべてのバックアップの暗号化：**転送時でも静止時でも、侵害されるとデータは読み取れないままとなります。
- **従業員の教育：**フィッシングの試みや、最初の侵害につながるその他のソーシャル エンジニアリングの手口を認識できるように、従業員を教育します。
- **定期的な脆弱性テスト：**テストを頻繁に行うことで、攻撃者が脆弱な領域を悪用する前に、このような脆弱な領域を特定してパッチを適用できます。

Dellは、これらの対応策と最先端のソリューションを組み合わせて、新たな課題に対応できる堅牢で対応力の高いインフラストラクチャを構築します。

セキュリティを強化する戦略的パートナーシップ

Dellは、Microsoft、CrowdStrike、Secureworksなどのサイバーセキュリティリーダー企業と連携しています。それぞれのパートナーシップにより、Dellのソリューションが強化され、高度な脅威インテリジェンス、エンドポイント モニタリング、包括的な対応戦略など、比類のない保護機能を提供しています。

Dell Professional Servicesを活用

デル・テクノロジーズのProfessional Servicesは、企業が複雑なサイバーセキュリティの課題に効果的に取り組むうえで役立つ専門知識とガイダンスを提供します。Dellのスペシャリストは、インシデント対応計画の策定からゼロトラスト アーキテクチャの実装まで、バックアップ侵入のような最新の脅威に対するクライアント環境のレジリエンスを確保します。

Dellでビジネス レジリエンスを強化

デル・テクノロジーズを選ぶと、事業の継続性を維持しながら、巧妙な攻撃者に先回りして対処することができます。Dellは、イノベーション、パートナーシップ、専門技術を通じて、組織が最も深刻なバックアップ侵入攻撃を防ぎ、検出して、このような攻撃から復旧できるようにします。

次のステップ

今すぐデル・テクノロジーズに連絡して、ビジネスを保護しましょう。当社はお客様の重要な資産を保護し、お客様の評判を守って、レジリエントな未来を築きます。

Dellはこれからも、デジタル時代における信頼を育み、組織の安全な運用と成功を収めるために必要なツール、知識、サポートを提供することに取り組んでまいります。

バックアップのレジリエンスはデル・テクノロジーズから始まります。今すぐ行動して将来を見据えた運用を実現し、サイバーセキュリティ体制の信頼性を高めましょう。

Dell.com/SecuritySolutionsで今日のサイバーセキュリティの重要な課題に対処する方法をご紹介しています

の詳細はこちら
Dellのソリューション

デル・テクノロジーズの
エキスパートへのお問い合わせ

他のリソースを表示

#HashTag で会話に参加

DELL Technologies