DELL Technologies

ランサムウェア：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

ランサムウェアとは

ランサムウェアは、身代金が支払われるまでコンピューター システムやデータへのアクセスを遮断する、悪意のあるソフトウェア（マルウェア）の一種です。深刻な問題を引き起こすサイバー攻撃の1つに数えられます。世界の組織の50%が過去1年間に少なくとも1回ランサムウェアの被害を受けています。ランサムウェア攻撃に伴う平均ダウンタイムは3週間に及び、深刻な業務中断を招いています。

増大するランサムウェア脅威

ランサムウェアは、身代金が支払われるまでコンピューター システムやデータへのアクセスを遮断する、悪意のあるソフトウェア（マルウェア）の一種です。深刻な問題を引き起こすサイバー攻撃の1つに数えられます。世界の組織の50%が過去1年間に少なくとも1回ランサムウェアの被害を受けています。ランサムウェア攻撃に伴う平均ダウンタイムは3週間に及び、深刻な業務中断を招いています。

ランサムウェアの仕組み

ランサムウェアは通常、誰かが悪意のあるリンクをクリックしたり、感染した添付ファイルを開いたり、侵害されたWebサイトにアクセスしたりすることで、組織に感染します。その後、システムに侵入してファイルを暗号化し、読み取り不能にします。一般的なランサムウェア プログラムは、復号化キーと引き換えに支払いを（多くの場合は暗号通貨で）要求するメッセージを表示します。身代金が支払われない場合、攻撃者はデータを削除したり公開したりすると脅迫することがあります。2017年に発生したWannaCry攻撃は、ランサムウェア攻撃の代表例と言えます。攻撃は世界中に急速に拡散して、病院、企業、政府機関に影響を及ぼし、経済に甚大な被害をもたらしました。Cyber Risk Management (CyRiM)とLloyd's of Londonによると、WannaCryウイルスによる世界経済への影響額は40億ドルから80億ドルに上り、わずか数日のうちに150か国で20万台以上のシステムが影響を受けました。

影響を受けた世界大手企業のうちの2社を挙げると、FedExはサービスの中断とクリーンアップによる3億ドルの損失を報告し、ルノー日産は複数の工場で生産を一時停止せざるを得なくなりました。ランサムウェア攻撃には、次のような隠れたコストが存在します。

- 会社のダウンタイムと生産性の損失
- 評判へのダメージ
- システムのリカバリーとパッチ適用のコスト
- 法規制上の罰金

ランサムウェア攻撃に直面した企業は、次の措置を講じなければなりません。

- 絶対に必要な場合を除き、支払いを行わない。攻撃者がアクセスを回復する保証はありません。
- バックアップがあれば、そこから復元する。
- 攻撃を当局に報告する。
- 将来の感染を防ぐための防御を強化する（ソフトウェアの継続的アップデート、スタッフのトレーニング、エンドポイント保護の使用など）。

© 2025 Dell Inc. その関連会社。

デル・テクノロジーズでランサムウェア攻撃に対抗

デル・テクノロジーズは、ランサムウェアのリスクを未然に防ぐための包括的で先進的なツールを提供します。

Dell Trusted Deviceによるエンドポイント セキュリティの強化

エンドポイントはランサムウェア攻撃の主要なエントリー ポイントになることが多く、エンドポイント セキュリティは特に重要な重点領域です。Dell Trusted Deviceにはハードウェア対応のセキュリティ機能が組み込まれており、パフォーマンスを損なうことなくシステムを保護できます。Dell SafeBIOSやSafeIDなどのソリューションでは、エンドポイント デバイスを不正アクセスから保護できます。Dell SafeDataでは、データを暗号化して、企業のファイアウォールの外側でも機密情報を保護できます。セキュリティがデバイスに直接組み込まれているため、企業はハードウェア レベルで保護を行い、攻撃者が足掛かりを得る機会を減らすことができます。

CrowdStrikeによるプロアクティブな検出

適切なツールを使用し、脅威をリアルタイムで検出して対応していれば、組織はランサムウェア攻撃を回避できます。Dellのソリューション ポートフォリオに付帯するCrowdStrikeは、AIと行動分析を活用した次世代のエンドポイント保護プラットフォームを提供します。このテクノロジーにより、不審なアクティビティーが攻撃に発展する前に特定して無力化できます。CrowdStrikeはDellのインフラストラクチャとシームレスに統合するため、ITチームは環境全体の可視性を維持しながら、脅威に迅速かつ効果的に対応できます。

Dell PowerProtectによる包括的なデータ保護

Dell PowerProtectの各種ソリューションは、ランサムウェア レジリエンスのバックボーンです。これらの高度なデータ保護ツールは、内外両方の脅威からエンタープライズ データを保護するように設計されています。不変バックアップなどの機能により、ランサムウェアによるデータの改ざん、削除、暗号化を防止し、高度な攻撃に直面しても信頼性の高いセーフティー ネットを構築します。例えば、Dell PowerProtect Cyber Recoveryヴォールトは、エアギャップ テクノロジーを使用して重要なデータをネットワークから隔離し、極めて巧妙な侵害を受けた際もデータを保護します。自動異常検出とインテリジェントなワークフローにより、組織は悪意のあるアクティビティーを早期に検出し、ランサムウェアが拡散する前に対応できます。

Dell PowerSwitch NetworkingとSmartFabric OSによる高度なネットワーク セキュリティとマイクロセグメンテーション

インフラストラクチャ全体で高度なネットワーク セグメンテーション、厳格なアクセス制御、リアルタイムのトラフィック分析を行うことで、ゼロデイ攻撃に対する防御を強化します。

Dellデータ保護サービスによる大規模なリカバリー

ランサムウェア対策においては、防止だけでなく、リカバリーも重要であることをDellは理解しています。Dellのデータ保護サービスでは、自動バックアップ/リカバリー ソリューションだけでなく、エキスパートによるコンサルティングも提供しており、企業は迅速にリカバリーを行い、ダウンタイムを最小限に抑えられます。リモート データ リカバリーやインシデント対応などのサービスにより、組織は危機がピークに達した状況で必要な支援を受けることができます。このような包括的なアプローチは、データの整合性を維持し、リカバリー時間を短縮し、業務の中断を防ぎます。

これらをはじめとするDellの豊富なソリューション ポートフォリオは、悪意のある内部関係者による脅威に対抗することを支援します。

パートナーシップによる強み

Dellの協働的なアプローチは、Dell独自のテクノロジーを超えて保護を拡張します。Dellは、CrowdStrikeやSecureworksといった大手サイバーセキュリティ企業とのパートナーシップを通じて、想定されるあらゆる攻撃ベクトルに対応する統合ソリューションのエコシステムを提供しています。こうしたソリューションを組み合わせることで、エンドツーエンドのセキュリティ カバレッジが確保され、企業は独自のリスク プロファイルに合わせた多層防御を構築できます。

Dellが選ばれる理由

デル・テクノロジーズは、単なるテクノロジー プロバイダーではなく、ランサムウェアとの戦いにおいて信頼できるパートナーです。イノベーション、専門技術、企業支援の取り組みを組み合わせ、進化する脅威に立ち向かうために必要なツールと自信を組織に提供します。エンドポイントの保護であっても、重要なデータの保護、迅速なリカバリーの達成であっても、Dellの製品とサービスは、運用の継続性を確保し、安心感をもたらします。

© 2025 Dell Inc. その関連会社。

レジリエントな未来を築くために

ランサムウェア攻撃は進化を続けていますが、デル・テクノロジーズをご利用いただくことで、その一歩先を行くことができます。高度なハードウェア、ソフトウェア、サービスをご活用になり、レジリエンス、適応性、信頼性に優れたサイバーセキュリティ フレームワークを構築してください。ランサムウェアに対抗するDellの包括的なソリューションで、データと業務を保護し、将来を見据えたビジネスを展開しましょう。

ビジネスのレジリエンスを確保するには、脅威の最新動向を把握し、新たな脅威について常に情報を得ることが不可欠です。デル・テクノロジーズのサイバーセキュリティ エキスパートは、新たな攻撃ベクトル（何を指していますか？）を常に監視し、製品とサービスの潜在的な脆弱性にプロアクティブに対処するよう努めています。これにより、当社は進化し続けるランサムウェアの脅威に対抗するための最新の保護を提供することができます。

企業は情報を常に把握することに加え、多層型のセキュリティ対策を講じる必要もあります。これは、ファイアウォール、マルウェア対策ソフトウェア、侵入検出システム、データ バックアップなど、さまざまなセキュリティ対策を導入することを意味します。防御戦略を多様化することで、1回の攻撃による影響を最小限に抑え、ランサムウェア攻撃が成功した場合でもビジネスを継続させることができます。

また、セキュリティ施策を定期的にテストしてアップデートすることも重要です（システムへのパッチ適用とポリシーのアップデートの両方）。ハッカーは、従来のセキュリティ対策を回避する新たな方法を絶えず探しているため、企業は防御策を定期的にテストし、必要に応じてアップデートして、常に先を行くことが重要です。これには、定期的な脆弱性評価、侵入テスト、パッチ管理の実施が含まれます。

ランサムウェアからビジネスを保護する上でもう1つ重要となるのが、サイバーセキュリティのベスト プラクティスに関する従業員教育です。多くのランサムウェア攻撃は、フィッシングEメールや悪意のあるリンクといったソーシャル エンジニアリング戦術を通じて開始されます。こうした脅威を検出して回避する方法を従業員に教育することで、攻撃が成功する可能性を大幅に減らすことができます。

さらに、ディザスター リカバリー計画を策定することで、ランサムウェア攻撃の影響を大幅に軽減できます。この計画には、重要なデータとシステムの定期的なバックアップの他に、攻撃への対応とリカバリーの明確な手順を含める必要があります。

こうしたプロアクティブな施策に加え、強固なインシデント対応計画を策定することも重要です。これには、ランサムウェア攻撃への対応における役割と責任の明確な定義、関係者への通知と被害軽減のための通信手順が含まれます。

最後に、ランサムウェア攻撃の最新動向や進歩について常に情報を得ることで、潜在的な脅威の一歩先を行くことができます。セキュリティ エキスパートによる業界レポートと最新情報を定期的に確認することで、ビジネスを保護するための新しいセキュリティ対策をプロアクティブに実装できます。

ランサムウェア攻撃の影響を受けないビジネスはありませんが、適切な戦略とツールを導入することで、このような攻撃のリスクと影響を最小限に抑えられます。サイバーセキュリティに対してプロアクティブなアプローチを取ることで、ビジネスを保護するだけでなく、お客様やステークホルダーとの信頼を築くこともできます。

今日のサイバーセキュリティの重要課題に対処する方法をご確認ください：**Dell.com/SecuritySolutions**

Dellのソリューションの詳細についてはこちら

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

© 2025 Dell Inc. その関連会社。All rights reserved.（不許複製・禁無断転載）。Dell、ならびにこれらに関連する商標およびDellが提供する製品およびサービスにかかる商標はDell Inc.またはその関連会社の商標です。またはその関連会社の商標または登録商標です。

DELL Technologies