DELL Technologies

ゼロデイ：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

増加するゼロデイ攻撃の脅威

ゼロデイ攻撃は急速に拡大しており、今日のサイバーセキュリティを取り巻く環境において、最も困難な課題の1つとなっています。こうした攻撃は、ソフトウェア プロバイダーやセキュリティ エキスパートには知られていない脆弱性を悪用するものであり、企業は準備が整っておらず、無防備な状態になっています。医療から金融まで、あらゆる業界の組織は、このような侵害に脆弱であり、多くの場合、金銭的にも運用においても深刻な影響を受けます。

デジタル トランスフォーメーションは加速しており、ゼロデイ攻撃はさらに頻繁かつ巧妙になっています。堅牢な保護のニーズは、かつてないほど大きくなっています。この脅威の重要な性質を理解しているデル・テクノロジーズは、革新的で拡張性のある防御を企業に提供し、企業が効果的にゼロデイ攻撃に対抗してリカバリーできるようにしています。

ゼロデイ攻撃とは

ゼロデイ攻撃は、ソフトウェアやハードウェアのまだ明らかになっていないセキュリティ脆弱性を、パッチまたは修正が利用可能になる前に悪用します。攻撃者は、時間的に有利となるチャンスを利用し、脆弱性が検出され対処される前に、往々にして広範囲のシステム停止を引き起こします。

ゼロデイ攻撃の仕組み

1. **脆弱性の検出：**ハッカーは、ソフトウェア アプリケーションやシステム内のコーディングの欠陥や隠れたバックドアを特定します。
2. **悪用方法の開発：**脆弱性を悪用するためにマルウェアが作成されます。攻撃者は、標的型フィッシング キャンペーンやマルウェアが仕込まれたWebサイトを使用して悪用を開始する可能性があります。
3. **攻撃の実行：**悪用方法が導入されると、システムが侵害され、データの窃盗や運用への干渉が実行される可能性が高まります。

一般的な手法

- ドライブバイ ダウンロードは、ユーザーがそれと知らずにマルウェアをインストールするよう誘導するものです。
- フィッシングEメールは、悪意のあるリンクやペイロード（コード本体）を配布して、脆弱性を悪用するものです。
- ファイルレス攻撃は、操作をすべてシステムのメモリー内で実行することで、検出を回避します。

こうした高度な攻撃ベクトルは、従来のシグネチャベースの検出ツールでは認識できないことが多いため、ゼロデイ攻撃は特に危険です。

ビジネスへの影響

予測が不可能で検出が遅れることから、ゼロデイ攻撃には重大なリスクが伴います。その結果は、いくつかの面で壊滅的なものになる可能性があります。

経済的損失

ゼロデイ攻撃が成功すると、規制違反による罰金からダウンタイム中の収益損失まで、膨大なコストがかかる可能性があります。たとえば、eコマース プラットフォームで未確認の脆弱性が悪用されると、清算手続きができなくなる可能性があり、売上に直接、影響が及ぼされることになります。

評判への影響

企業の社会的イメージが、取り返しのつかないほど傷つく可能性があります。機密情報の漏洩やサービス停止があると、お客様からの信頼が失われます。

業務の中断

対処されていない脆弱性によってシステムが麻痺することも多く、生産性の低下、プロジェクトの遅延、ビジネス チャンスの逸失につながります。

実例

ある大手医療機関は、パッチを適用していない医療デバイス ソフトウェアを標的としたゼロデイ攻撃の被害を受けました。この攻撃により、主な業務が止まり、患者データが漏洩し、組織はリカバリーに**数百万ドル**をかけましたが、患者からの信頼は損なわれました。

驚くべき統計

2023年のPonemonの調査によると、ゼロデイによる侵害の割合は約80%に及ぶとのことです。

ゼロデイ攻撃は一貫して脆弱性悪用の**70%**以上を占めている

出典：2024年：iMandiant「M-Trends」

デル・テクノロジーズでゼロデイ攻撃に対抗

デル・テクノロジーズは、業界をリードするソリューションを提供し、企業がゼロデイ攻撃を積極的に防御しながら、そのような侵害を受けた後、迅速にリカバリーできるように支援しています。

サーバーおよびストレージのセキュリティ ソリューション

Dellのサーバーおよびストレージのセキュリティ ソリューションは、次のような追加の保護レイヤーを提供します。

- セキュア サーバーが、不正なアクセス試行を監視してブロックします。
- データのバックアップおよびリカバリー システムが、最悪のシナリオであっても、重要な情報にアクセスできるように、またそれらの情報に影響が及ばないように維持します。

Dell Trusted Deviceでエンドポイントを強化

エンドポイントは、攻撃者にとって重要なエントリー ポイントです。Dell Trusted Deviceには高度なセキュリティ対策が組み込まれており、エンドポイントを未確認の脅威から確実に保護します。

- **SafeBIOS**は、ファームウェアを不正操作から保護し、システムの整合性をゼロから確保します。
- **SafeID**は、認証プロセスを保護することでユーザーの認証情報を保護します。
- **SafeData**は、静止データと転送中の機密データを暗号化し、傍受や悪用が発生した場合にそれらのデータを使用できなくします。

CrowdStrikeによるプロアクティブな脅威検出

CrowdStrikeは、高度な分析とAIを活用してエンドポイント アクティビティーを監視し、ゼロデイ攻撃を示している可能性のある異常な動作を検出します。そのプロアクティブな脅威検出により、脆弱性による損害が広がる前に迅速に対応できるようになります。

たとえば、CrowdStrikeを使用しているある通信プロバイダーは、ネットワーク トラフィックの異常を早期に検出し、お客様のサーバーで発生する可能性のあるゼロデイ攻撃を軽減しました。

Dell PowerProtectソリューション

Dell PowerProtectは、堅牢で不変のバックアップと、分離されたリカバリー オプションを提供します。ゼロデイ攻撃を受けた後も、企業は迅速かつ効率的に業務を再開し、ビジネスの継続性を維持し、重要な顧客データを保護することができます。

たとえば、PowerProtectを利用しているある大手小売チェーンは、ゼロデイ脆弱性に起因するランサムウェア攻撃を受け、暗号化済みファイルへの侵害を受けましたが、それらのファイルをリカバリーさせて長期にわたるダウンタイムを回避しました。

Dell PowerSwitchネットワーキングと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、ネットワークの高度な区分化、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実行し、ゼロデイ攻撃に対する防御を強化します。

多層型セキュリティ アプローチの重要性

真のセキュリティには、複数のソリューションが必要です。多層型戦略は、テクノロジー、プロセス、人材を組み合わせて包括的な保護フレームワークを形成します。

防衛強化のための重要なアクション

- **ゼロトラスト原則の採用：**ネットワークへのアクセスを試みるすべての個人とデバイスを確認します。
- **高度な暗号化の実装：**暗号化プロトコルを使用して、移動中のデータと保存中のデータの両方を保護します。
- **従業員の教育：**従業員に詳細なトレーニング セッションを提供して、フィッシング攻撃やソーシャル エンジニアリング戦術を認識する方法を教えます。
- **定期的なシステム テスト：**一貫性のある侵入テストと脆弱性スキャンを実施して、新しい脅威に防御が適応することを確認します。

デル・テクノロジーズは、こうした実践と高度なセキュリティ ソリューションとを組み合わせて、組織がゼロデイ脆弱性に効果的に対処できるようにします。

サイバーセキュリティを強化するパートナーシップ

Dellは、業界リーダーである**Microsoft**、**CrowdStrike**、**Secureworks**とのコラボレーションにより、お客様が最先端のセキュリティ インテリジェンスとツールにアクセスできるようにします。

- **Microsoft**は、Dellのソリューションとシームレスに統合され、システム全体の互換性とプロアクティブな保護メカニズムを確保します。
- **CrowdStrike**は、高度なエンドポイント脅威インテリジェンスを提供し、潜在的なゼロデイ攻撃を検出します。
- **Secureworks**は、継続的なモニタリングとエキスパートによる修復を提供し、リアルタイムの攻撃に対応します。

Dell Professional Servicesを活用する

Dell Professional Servicesでは、コンサルティング、実装、リカバリーの幅広く包括的な支援を提供し、企業がゼロデイ脅威に関わるリスクに対処し、影響を軽減できるよう支援します。Dellは、インシデント対応からサイバーセキュリティ ロードマップの立案まで、組織の長期的なレジリエンスの実現を支援します。

レジリエントな未来を築くために

デル・テクノロジーズに投資することにより、優れたテクノロジーを提供するパートナーを持てるだけでなく、安心を得ることもできます。Dellは、最先端のソリューション、戦略的パートナーシップ、比類のない専門技術を通じて、最も高度なゼロデイ攻撃であっても、その予測、検出、リカバリーができるように組織を支援します。

ビジネスを保護し、評判を守り、予測不可能なデジタル環境で成功を収めるために、今すぐデル・テクノロジーズにお問い合わせください。Dellが将来の脅威から守ります。

デル・テクノロジーズは、最も重要なものを保護するように設計されたセキュリティ ソリューションとサービスを通じて、進化するゼロデイ攻撃の課題に企業が先手を打てるようにします。これによって企業は自信を持つことができます。

今日のサイバーセキュリティの最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

DELL Technologies