DELL Technologies

デル・テクノロジーズでサプライ チェーンのサイバー攻撃を防御

概要

事業運営のグローバル化と相互連携性の高まりにより、組織はサプライ チェーンのサイバー攻撃による脅威の増大に直面しています。この高度な攻撃は、製造から導入までのハードウェアのライフサイクルとサードパーティー製ソフトウェアでの脆弱性を悪用するものです。これにより、悪意のある攻撃者は、信頼できるアプリケーションやアップデートを通じてシステム全体を侵害します。このようなインシデントは、壊滅的な経済的損失をもたらすだけでなく、評判を低下させ、大規模な業務中断を引き起こす可能性があります。

こうした脅威の影響は極めて深刻です。サプライ チェーン攻撃は、重大な損害が発生して初めて明らかになることが多いため、プロアクティブな防御戦略が不可欠です。Dellは、高度なエンドポイント保護、プロアクティブなモニタリング、包括的なサーバーおよびデータ セキュリティ ソリューションにより、企業がサプライ チェーンをエンドツーエンドで保護できるよう支援します。組織は、テクノロジー、パートナーシップ、専門技術を導入することで、レジリエンスを高め、エコシステム内で固有の脆弱性から企業自体を守ることができます。

サプライ チェーンのサイバー攻撃の脅威の増大

サプライ チェーン攻撃は、近年大幅に増加しています。攻撃者は、製造、出荷、導入の過程で物理デバイスを改ざんしたり、ソフトウェア プロバイダーの弱点を探し出したりすることで、悪意のあるコンポーネントやコードを注入する手段や、システムを破壊する手段、機密データを引き出す手段を得ます。被害の範囲は、小規模企業からグローバル企業まで多岐にわたります。この攻撃の被害を受けると、深刻な経済的損失、顧客の信頼の低下、法的な制裁などの結果を招きます。デル・テクノロジーズはこのような危険性の増大を認識しており、この攻撃の壊滅的な影響を軽減するための予防措置を提言しています。

サプライ チェーンのサイバー攻撃を理解する

ハードウェア サプライ チェーン攻撃の攻撃方法

1. **製造段階：**攻撃者はハードウェアの組み立て中に悪意ある構成部品を混入させます。多くの場合、侵害されたサプライヤーを利用します。
2. **出荷段階：**デバイスが輸送中に奪取されて改ざんされ、有害なファームウェアやハードウェアの改造が仕込まれます。
3. **導入とアクティベーション：**侵害されたハードウェアが組織のネットワークに接続されると、攻撃者は機密データへのアクセスを乗っ取ったり、バックドア操作を可能にしたりします。

ソフトウェア サプライ チェーン攻撃の攻撃方法

1. **初期侵害：**サードパーティー ソフトウェア ベンダーへの侵害は、多くの場合、フィッシング、パッチが適用されていない脆弱性、内部関係者の脅威を通じて引き起こされます。
2. **コード操作：**悪意のある攻撃者が配布を目的としたソフトウェアにマルウェアやバックドアなどの有害な要素を注入します。

3. **エンドユーザーへの拡散：**侵害されたソフトウェアを企業がインストールまたはアップデートした結果、エンドユーザーが意図せず悪意のあるコンポーネントをダウンロードすることになります。

一般的な手法：ハードウェア

- **ファームウェア操作：**導入後にアクティブになる悪意あるコードを埋め込みます。
- **ハードウェアの改ざん：**密かに仕込まれたコンポーネントを統合してデータを監視または流出させます。
- **信頼されているサプライヤーの悪用：**プロセスのセキュリティが不十分なサードパーティー ベンダーを利用します。

一般的な手法：ソフトウェア

- **コンポーネントのハイジャック：**サードパーティーのライブラリーまたはフレームワークに悪意のあるコードを感染させます。
- **アップデートでの注入：**公式ソフトウェア アップデートを改ざんし、エクスプロイトを仕込みます。
- **依存関係の混乱：**組織が安全でないパッケージ依存関係に頼っていることを悪用します。

ビジネスへの影響

財務的な影響

多くの場合、サプライ チェーンを標的とした攻撃を受けると、法的罰金、システム リカバリー費用、顧客への補償など、多大なコストが生じます。あるグローバルIT管理企業が巻き込まれた注目度の高いインシデントでは、損失額が7,000万ドルを超えました。このことは、この侵害が深刻な経済的損失をもたらす可能性があることを示しています。

業務の中断

マルウェアの侵入によってシステムが破損または無効化されると、一般的にダウンタイムが大幅に増加し、組織の生産性が低下して、プロジェクト成果物の遅延が生じます。

評判への影響

現在のビジネスにとって、ソフトウェア パートナーへの信頼は極めて重要です。組織のソフトウェア製品に関連するサプライ チェーンの侵害が発生すると、評判を損ない、顧客のロイヤルティを失う可能性があります。

実際の事例：ハードウェア/ソフトウェア

あるグローバルな電子機器メーカーは、そのサプライ チェーン内で侵害されたコンポーネントを発見しました。これは、広範囲にわたるシステム障害につながりました。この攻撃により、**4,500万ドル**を超えるリカバリー費用と訴訟費用が発生し、サプライヤーとの関係に壊滅的なダメージが生じました。

SolarWindsへの攻撃は、最も悪名高いソフトウェア サプライ チェーン攻撃の1つです。同社のOrion製品の侵害は、政府機関やFortune 500企業など、世界中の組織が感染する結果をもたらしました。損害額は**9,000万ドル**を超え、サプライ チェーンの脆弱性が極めて広範囲な影響をもたらしたことが明らかになりました。

サプライ チェーン攻撃に関するデル・テクノロジーズの専門知識

デル・テクノロジーズの幅広いセキュリティ ソリューション ポートフォリオを利用することで、企業は進化するサイバーリスクに先手を打つことができます。

Dell Secure Component Verification (SCV)

Secure Component Verification (SCV)は、デル・テクノロジーズのサプライ チェーン セキュリティ戦略に不可欠な要素で、さまざまなDellソリューションのハードウェア コンポーネントの信頼性と整合性を確保するよう設計されています。SCVは、製造から配送および導入の時点まで、暗号化を用いたシステム コンポーネントの検証を提供します。デル・テクノロジーズは堅牢なサプライ チェーン セキュリティを提供して、製造工場から導入までシステムが改ざんされることなく、安全な状態を保てるようにします。その結果、Dellのお客様の全体的なセキュリティ、信頼性、パフォーマンスが高まります。

Dell Trusted Deviceでエンドポイントを保護

Dell Trusted Deviceは、ハードウェア レベルとファームウェア レベルでセキュリティを統合し、改ざん防止システムを構築します。

- **SafeBIOS：**起動時にファームウェアの整合性を確保し、不正な構成変更を防止します。起動時にファームウェアの整合性を検証して、侵害されたシステムが起動されないようにします。
- **SafeID：**ハードウェア レベルで認証情報を保護し、不正アクセスを防止します。認証キーを安全に管理することでログイン認証情報を保護し、不正ユーザーのアクセスを遮断します。
- **SafeData：**機密性の高いビジネス ファイルをエンドツーエンドで暗号化できるようにして、悪用できるデータを引き出そうとする試みを阻止します。

CrowdStrikeによるプロアクティブな脅威検出

CrowdStrikeはDellのテクノロジーと連携して、悪意のあるソフトウェアの動作に関するリアルタイムのインサイトを提供します。

- **振る舞いベースの脅威検出分析：**ハードウェアとファームウェアの動作を監視して改ざんの兆候を見つけ出し、異常なソフトウェア アクティビティーを検出して、マルウェアの導入を防止します。
- **即時対応ツール：**AIが侵害されたシステムを隔離し、ネットワーク内でのラテラル ムーブメントを阻止します。
- **AIベースの脅威修復：**脅威を積極的に特定して分離し、エンタープライズ システム内での水平展開を防ぎます。
- **統合機能：**DellとCrowdStrikeのツールを使用して、ハイブリッド環境とマルチクラウド環境を包括的に保護します。

Dellのサーバーおよびストレージ ソリューションによるセキュリティの強化

Dell PowerEdgeサーバー ファミリーには、ミッションクリティカルなソフトウェア プラットフォームを保護するための高度な保護機能が組み込まれています。Dell PowerStoreなどのストレージ システムは、業界をリードするアプリケーションとデータの暗号化機能を備えています。

- **安全なサーバー ファームウェア：**ハードウェア レベルの不正な変更を監視してブロックします。
- **分離ネットワークのモニタリング：**サプライ チェーンの改ざんを示す異常を検出します。
- **不変バックアップ：**プライマリー ストレージが侵害された場合でもリカバリー ポイントを保護します。
- **リカバリー ヴォールト：**分離された環境により、侵害されたシステムから発生する連鎖的な障害に対する保護が実現します。

リスクを軽減する多層型アプローチ

Dellは、テクノロジー、人事慣行、最新のプロセスを組み合わせた包括的な戦略を採用することを企業に奨励しています。

戦略的ステップ

- **サプライ チェーンの可視性の向上：**すべてのベンダーに対し、厳格なセキュリティ基準を遵守し、すべての段階でハードウェアを認定することを要求します。
- **高度な暗号化の実装：**高度なプロトコルを使用してあらゆるレベルでデータを保護し、ハードウェアが侵害された場合でもアクセスを制限します。
- **ゼロトラスト ポリシーの採用：**検証なしでデバイス、アプリケーション、ユーザーが自動的に信頼を得ることがありません。
- **セキュア コーディング標準：**ソフトウェア パートナーと協力して、プラグイン、API、統合に関する厳格なガイドラインを適用します。
- **アクティビティーの監視と定期的な監査の実施：**可視性監査を頻繁に実施することで、サードパーティー サービス全体の整合性を確保します。
- **定期的なテストの実施：**侵入テストとファームウェア評価を導入して、デバイスの整合性を継続的に検証します。
- **従業員の教育：**疑わしい動作を示すコンポーネントやパッケージを把握できるようにチームをトレーニングします。

Dell Professional Servicesでビジネス レジリエンスを確保する仕組み

DellのProfessional Servicesは、企業が堅牢なサプライ チェーン防御を導入できるよう支援します。経験豊富なサイバーセキュリティ エキスパートのチームが、組織固有のニーズに合わせてカスタマイズされた評価、トレーニング、脅威対応戦略を提供します。

- **実装ガイダンス：**ベンダー環境全体で、ゼロトラストと監査済みのプロバイダー プラクティスを戦略的に調整します。
- **インシデント対応：**悪意のあるインシデントが発生した場合に、ビジネスを迅速に復旧できるようにします。

Dellでエンタープライズ システムの未来に備える

サプライ チェーンのサイバー攻撃は、新しい脅威が巧妙化していることを実証しています。企業は、侵害を防ぐだけでなく、インシデントが発生した場合に迅速に復旧できる保護対策を必要としています。デル・テクノロジーズと提携することは、最先端のツール、戦略的な専門知識、信頼できる協力者のネットワークを利用できることを意味します。

次のステップ

デル・テクノロジーズが策定するベスト プラクティスを導入して、機密性の高い資産を保護し、運用の信頼性を効率化しましょう。エンタープライズ システムのライフラインを保護する準備を進めているなら、今すぐお客様に合わせたコンサルティングをご利用ください。

サプライ チェーンのサイバーセキュリティが進化する中、デル・テクノロジーズは信頼性、適応性、イノベーションを体現しています。今日の取り組みが、明日の成功を守ります。

より安全な未来は、デル・テクノロジーズから始まります。最も重要なものを守るお手伝いなら、デル・テクノロジーズにお任せください。

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

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