DELL Technologies

悪意のある内部関係者：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

悪意のある内部関係者による攻撃の脅威の増大

悪意のある内部関係者による攻撃は、今日のビジネス環境において最も差し迫ったサイバーセキュリティの脅威の1つとなっています。悪意のある内部関係者は、外部の脅威とは異なり、組織内である程度の信頼を確立し、アクセス権を持っているため、その行動は特に有害であり、検出が困難です。機密データへのアクセスからシステムの破壊まで、内部関係者による攻撃は重要な業務を妨害し、財務面や評判に深刻な影響を及ぼす可能性があります。

デル・テクノロジーズは、この攻撃がもたらす危険性の増大を認識しており、企業が悪意のある内部関係者のリスクを特定、防止、軽減できるよう支援する、革新的で拡張性のあるソリューションを開発しています。Dellは、最先端のテクノロジーとエキスパートによるサービスを組み合わせることで、組織が内部からの脅威に先回りして対処できるよう支援します。

悪意のある内部関係者による攻撃とは

悪意のある内部関係者による攻撃とは、組織内の個人が、個人的な目的、金銭的な目的、または競争上の目的のために、アクセス権を悪用してデータを侵害したり、業務を中断したり、機密情報を抽出したりする攻撃です。この個人は、従業員、請負業者、パートナー、または会社のシステムやネットワークへの正当なアクセス権を持つ人物である可能性があります。

悪意のある内部関係者による攻撃の攻撃方法

悪意のある内部関係者は、信頼されている立場を悪用して従来のセキュリティ防御を回避します。一般的な手法には次のとおりです。

1. **データの盗難：**顧客の機密データ、知的財産、財務記録を引き出す行為です。
2. **妨害行為：**ITシステムを故意に破壊することで、業務運営を妨害し、評判を失墜させます。
3. **認証情報の悪用：**盗難または悪用された認証情報を使用して、アクセス権限を昇格させたり、ダミー アカウントを作成したりします。
4. **外部の攻撃者との連携：**金銭的利益と引き換えに、アクセスや機密情報を外部のサイバー犯罪者に提供します。

悪意のある内部関係者は、信頼と内部の知識という二重の強みを持つため、外部の攻撃者以上に大変危険な存在です。

ビジネスへの影響

悪意のある内部関係者による攻撃の被害は広範囲に及び、金銭的損失を超えた損害を引き起こします。企業は次のような被害を受ける可能性があります。

経済的損失

機密情報の盗難、詐欺、妨害行為が、数百万ドルに及ぶ収益の損失とリカバリー費用につながるおそれがあります。

業務の中断

システムの妨害行為やデータ破壊によって業務が停止し、遅延、機会の損失、生産性の低下につながるおそれがあります。

評判へのダメージ

内部関係者による侵害や攻撃は、クライアントとステークホルダーの信頼を損ない、顧客ロイヤルティと市場の認識に影響を及ぼします。

法令遵守違反

医療や財務といった機密データを扱うなど、業界によっては、内部関係者による攻撃によって多額の罰金や罰則が科される可能性があります。

実例

2020年に、大手金融機関に勤務していたIT請負業者が、重要なシステム構成を意図的に削除し、**10時間**以上にわたってネットワークを停止させました。この妨害行為は、**数百万**ドルの経済的損失、多額のリカバリー費用、評判への悪影響をもたらしました。このようなインシデントは、内部関係者の脅威がもたらす破壊的な可能性を示しており、堅牢な検出と防止対策の緊急性を強調しています。

推定コスト

2024年にPonemon Instituteが実施した調査によると、内部関係者関連のインシデントの平均コストは**499万ドル**と推定されており、すべての侵害の約**55%**を占めています。この数値は、検出、リカバリー、軽減にかかる費用を考慮したものであり、組織が内部関係者リスクに対する予防的な防御対策に投資する必要性を浮き彫りにしています。

83%

過去1年間に1件以上の内部関係者攻撃を報告した組織の割合

出典：Cybersecurity Insidersのレポート（2024年）

デル・テクノロジーズで悪意のある内部関係者による攻撃に対処

デル・テクノロジーズは、悪意のある内部関係者の脅威に対処するためのツールとサービスの包括的なエコシステムを提供し、組織が不測の事態に対して準備できるようにします。

Dell Trusted Deviceでエンドポイントを保護

多くの場合、エンドポイントは内部関係者の脅威の侵入経路となります。Dell Trusted Deviceは、最先端のセキュリティ機能をハードウェアに統合してエンドポイントを強化し、機密データを保護します。

- **Dell SafeBIOS：**ファームウェアの整合性を確保し、ハードウェア レベルでシステム操作をコントロールしようとする試みを阻止します。
- **SafeID：**認証情報データを保護し、不正アクセスや認証情報の不正使用を防止します。
- **SafeData：**機密データをエンドツーエンドで暗号化し、傍受または抽出された情報を悪意のある内部関係者が読み取れないようにします。

これらのソリューションを導入することで、脅威が内部から発生しているか外部から発生しているかにかかわらず、エンドポイントを確実に保護できます。

CrowdStrikeによるプロアクティブな脅威検出

内部関係者の脅威を特定するには、ユーザーの行動を可視化して監視する必要があります。Dellのソリューションに統合されているCrowdStrikeは、AIと行動分析を活用して、内部関係者の脅威を示す異常を検出します。

たとえば、営業時間外の異常なデータ転送や、ネットワークの重要な領域への不正アクセスには直ちにフラグが付けられ、迅速に対応できるようになります。米国のある医療機関は、プロアクティブな脅威検出を活用することで、従業員による患者データの漏洩を特定して未然に防ぎ、大きな損失につながる侵害を阻止しました。

Dell PowerProtectによるデータ保護の強化

Dell PowerProtectは、安全なバックアップ、エアギャップされたストレージ、重要なデータの不変コピーによって、堅牢な防御線を築きます。機密情報を改ざんや削除から確実に守ることで、データの整合性を標的とした内部関係者による攻撃の効果がなくなる可能性があります。

ある製造企業で、不満を抱いている従業員が設計ファイルを破壊しようと試みた事例がありました。この企業は、Dell PowerProtectのリカバリー ヴォールトにより、数時間以内に業務を再開。中断を回避し、事業の継続性を維持することができました。

Dell Professional Servicesによる迅速なインシデント リカバリー

内部関係者の脅威がインシデントになった場合には、迅速なリカバリーが不可欠です。リモート データ リカバリーやインシデント対応を含むDellのProfessional Servicesにより、企業はデータとシステムを迅速に復旧できます。Dellのエキスパートが、ダウンタイムを最小限に抑え、影響を軽減するプロセスを主導します。

これらは、悪意のある内部関係者の脅威に対処するためのDellのソリューション ポートフォリオのほんの一例にすぎません。

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に高度なネットワーク区分化、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導入することで、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

内部関係者のリスクに対し効果的に防御するには、多層的な保護が必要です。多層型セキュリティ戦略を導入すれば、脆弱性が弱点となることがありません。重要なステップは次のとおりです。

防御を強化するための重要なステップ

- **ゼロトラストの原則：**すべてのアクセス リクエストを継続的に検証し、境界内であっても本質的に信頼できるエンティティがないと想定します。
- **ロールベースのアクセス制御(RBAC)：**従業員が、各自のロールに必要なシステムとデータのみにアクセスできるように制限します。
- **高度な暗号化ソリューション：**静止時と転送時のデータを暗号化し、データの盗難を効果的に無効化します。
- **従業員の意識向上とトレーニング：**不注意で悪意のあるアクティビティーに関わることがないようにするため、定期的なセキュリティ意識向上プログラムを実施します。
- **定期的なシステム テスト：**防御が信頼できる状態を確実に維持できるよう、侵入テストと脆弱性スキャンを実施します。

これらの対応策は、Dellのソリューションによって強化され、悪意のある内部関係者に対する強力で包括的な保護フレームワークを構築します。

戦略的パートナーシップによる防御の強化

Dellは、**CrowdStrike**や**Secureworks**などの業界をリードするサイバーセキュリティ プロバイダーと提携して、ソリューションをさらに強化しています。CrowdStrikeはエンドポイント セキュリティを強化し、侵害の兆候に関する貴重な脅威インテリジェンスを提供します。Secureworksは高度な脅威検出および対応サービスを提供します。こうした連携により、Dellのお客様は、統合された最先端テクノロジーのエコシステムの恩恵を受けることができます。

サイバーセキュリティでデル・テクノロジーズを選ぶ理由

デル・テクノロジーズは、多層型サイバーセキュリティ ソリューションのゴールド スタンダードを確立し続けています。企業は、Dellの業界をリードする専門知識、深いパートナーシップ、今日の進化する脅威の状況に適応する革新的な製品群によるメリットを享受できます。エンドポイント セキュリティから内部関係者の検出、インシデント リカバリーにいたるDellの包括的なレジリエンス フレームワークは、信頼を高め、成長を可能にします。

デル・テクノロジーズのソリューションでレジリエントな未来を構築

デル・テクノロジーズの包括的で拡張性に優れたソリューションで、悪意のある内部関係者の脅威からビジネスを守りましょう。Dellと提携することで、業務を守るだけでなく、事業の継続性の確保、顧客からの信頼向上、将来を見据えた組織態勢の実現が可能になります。今すぐプロアクティブな防御の導入に関する詳細について、お問い合わせください。

デル・テクノロジーズは、お客様の信頼できるパートナーとして、内部関係者の脅威に対処し、重要な資産を保護して、ダイナミックなデジタル環境でビジネスを成功に導きます。成功をもたらすセキュリティの未来は、Dellから始まります。

Dell.com/SecuritySolution 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

他のリソースを見る

#HashTag で会話に参加

DELL Technologies