DELL Technologies

中間者(MITM)攻撃：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

中間者(MITM)攻撃の脅威の増大

中間者(MITM)攻撃は、依然として最も高度で危険なサイバーセキュリティの課題の1つです。悪意のある攻撃者が検出されることなくプライベート通信を傍受して改ざんするこの攻撃は、業界を問わずあらゆる規模の企業を標的としています。eコマース プラットフォームから金融機関にいたるまで、このリスクと無関係でいられる組織はありません。多くの場合、MITM攻撃はデータの盗難、金融詐欺、風評被害につながるため、デジタル化が進む現在の状況において強力な脅威となっています。

デル・テクノロジーズは、企業がこの高度な脅威から自社を保護する際に直面する固有の課題を理解しています。Dellは、革新的で拡張性のあるセキュリティ ソリューションを提供することで、組織がMITMの脅威を無力化し、資産を保護して、ビジネスの整合性を維持できるよう支援します。

中間者攻撃(MITM)とは

中間者(MITM)攻撃では、サイバー犯罪者が2者間（従業員と企業のサーバー間、顧客とビジネスWebサイト間など）の通信を密かに傍受します。攻撃者の目的は、機密データの盗難から悪意のある目的での通信の操作までさまざまですが、いずれの場合でも信頼とセキュリティを侵害する結果に行き着きます。

一般的なMITMの手法

攻撃者が使う最も一般的な手法には、次のようなものがあります。

Wi-Fiの盗聴：サイバー犯罪者は、セキュリティ保護されていない、または侵害されたパブリックWi-Fiネットワークを悪用して通信を傍受します。

DNSスプーフィング：攻撃者はDNSレコードを改ざんしてユーザーを不正なWebサイトに再ルーティングし、怪しまれることなく機密情報を収集します。

セッション ハイジャック：攻撃者はアクティブなセッションの認証情報を入手して、プライベート アカウントへ不正にアクセスします。

SSLストライピング：この手法では、安全なHTTPS接続を脆弱なHTTP接続にダウングレードして、機密情報を流出させます。

こうした適応性により、MITM攻撃は特に悪質性が高いといえます。表面的には正常に見える日常的なビジネス トランザクションややり取りを悪用するためです。

ビジネスへの影響

MITM攻撃の波及効果は、差し迫ったインシデントをはるかに超えて広がります。最も有害な影響には次のようなものがあります。

収益の損失

多くの場合、認証情報の盗難や業務への侵害は、直接的な損失からリカバリー コストにまで及ぶ経済的な負担をもたらします。

業務の妨げ

攻撃への対処に時間とリソースが費やされるため、重要なビジネス機能が損なわれ、生産性と成長に影響を及ぼします。

信頼の低下

個人情報が侵害されると、顧客からの信頼が急速に低下し、長期的な評判の低下につながるおそれがあります。

規制による悪影響

厳格なコンプライアンス要件が定められている業界で事業を展開している企業は、データ侵害の発生後に罰金や制裁を受ける可能性があります。

実例

ある世界的な小売企業で、暗号化されていないオンライン決済プラットフォームがSSLストライピング攻撃の被害を受けたという憂慮すべき事例があります。攻撃者は、チェックアウト手続き中の顧客からクレジットカード情報を傍受しました。Dellのエンドポイント保護ツールを含む迅速な検出と戦略的なセキュリティ対策により、この企業は攻撃を阻止し、長期的な損害を軽減できました。この事例では、差し迫ったリスクと、階層型防御の必要性が極めて高いことが浮き彫りになりました。

359億件

判明している世界のデータ侵害の件数

出典：PureWLのレポート（2024年5月）

デル・テクノロジーズでMITM攻撃に対処

デル・テクノロジーズは、MITMのリスクを未然に阻止するように設計された包括的で先進的なツールを組織に提供します。

Dell Trusted Deviceでエンドポイントを保護

エンドポイントは、MITMの脅威が頻繁に発生する場所なので、優先して保護すべき対象となっています。DellのTrusted Deviceは、最先端のセキュリティ機能をハードウェアに直接組み込みます。例：

- **Dell SafeBIOS：**ブート シーケンスの不正な改ざんを防ぎ、システムの整合性を確実に守ります。
- **SafeID：**ユーザー認証データの保護により保護を強化し、認証情報の盗難に対する防御を形成します。
- **Dell SafeData：**企業のファイアウォールの内外で機密情報を保護するエンドツーエンドの暗号化機能を提供し、傍受されたデータを読み取ることができないようにします。

多くのグローバル企業では、エンドポイント システムの信頼性を強化するためにこれらの機能が導入されています。たとえば、ある多国籍製造企業は、会社のノートパソコンを狙ったMITM攻撃からテレワーク社員を守り、リスクの高い出張のような状況でも安全な接続を確保するために、Dell Trusted Deviceを使用しています。

CrowdStrikeによる高度な検出

MITMの脅威をリアルタイムで検出して対応することは非常に重要です。Dellのエコシステムに統合されたCrowdStrikeは、AIと行動分析を活用して疑わしいアクティビティーを監視し、無力化します。継続的なモニタリングで、脅威が隠れていることが多いハイブリッド環境全体を確実に保護します。異常を事前に特定することで、企業はMITM攻撃の可能性を排除し、被害を未然に防ぐことができます。

ある金融機関の事例では、高度な検出機能を使用して、顧客向けポータルへの侵入を検出し、抑制することができました。このプラットフォームのAIがSSLストライピングの兆候を示す異常なネットワーク アクティビティーを特定し、その結果、迅速な修復が可能になりました。

Dell PowerProtectによるデータ保護の強化

高度な防御を導入している組織であっても、侵害が発生する可能性はあります。こうした状況に有効なのがDell PowerProtectです。不変性やエアギャップされたストレージなどの機能により、攻撃中に重要なビジネス データが改ざん、破壊、アクセスされることを防ぎます。PowerProtect Cyber Recoveryヴォールトは、機密データをプライマリー ネットワークから分離することでセキュリティを強化。最悪のシナリオでも機密情報が変更されることなく、リカバリー可能な状態で維持されます。

このテクノロジーは、DNSスプーフィング攻撃を受けたある医療機関で大きな助けとなりました。この医療機関は、PowerProtectの不変バックアップとリカバリー ヴォールトを活用することで、データを失うことなく迅速に業務を復旧しました。

迅速な対応とリカバリー サービス

Dellのデータ保護サービスは、侵害が発生した場合にエキスパートによる迅速な復旧を行い、Dellのテクノロジーを補完します。リモート データ リカバリーからインシデント対応まで、これらのソリューションはダウンタイムを低減し、業務の中断を最小限に抑えます。一刻を争う状況では、信頼できるパートナーの存在が、企業の確実な復旧を可能にします。

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。

多層アプローチによるセキュリティの強化

MITM攻撃に完全に対処するには、組織に多面的なセキュリティ戦略を導入する必要があります。デル・テクノロジーズは、次の実行可能なステップを重視しています。

- **ゼロトラストの原則の採用：**企業ネットワークの内外で、すべてのアクティビティーとユーザー アクセスをあらゆるポイントで検証します。
- **高度な暗号化の使用：**すべての通信でエンドツーエンドの暗号化を行うことで、傍受されたデータを攻撃者が使用できないようにします。
- **多要素認証(MFA)の実装：**MFAはシステムの認証を強化し、不正アクセスの脆弱性を大幅に軽減します。
- **従業員の教育：**フィッシングの試み、疑わしいWi-Fiの使用、未検証のリンクなどのリスクをハイライトすることで、従業員の警戒態勢を高めます。
- **定期的なシステム テスト：**侵入テストとアップデートを頻繁に行うことで、脆弱性を特定し、防御対策を最新の状態に保つことができます。

Dellの総合的なセキュリティ製品とこれらの対応策を組み合わせることで、進化する脅威に対する強力で適応性に優れた防御を築くことができます。

戦略的パートナーシップの価値

デル・テクノロジーズは、CrowdStrikeやSecureworksなどの主要なサイバーセキュリティ企業と連携することで、サービスをさらに強化しています。このようなパートナーシップを通じて専門技術を統合することで、Dellはあらゆる攻撃ベクトルに対処できます。たとえば、CrowdStrikeはDellのプラットフォームに脅威インテリジェンスを組み込んで、エンドポイント保護を強化します。Secureworksは進化するリスクに関する実用的なインサイトを提供し、継続的に準備し、適応できるようにします。

Dell Technologies Advantage

デル・テクノロジーを選ぶことは、サイバーセキュリティ イノベーションにおける信頼できるリーダーと提携することを意味します。Dellのエンドツーエンド ソリューションは、エンドポイント保護、データ リカバリー、協働パートナーシップのいずれを通じても、企業が攻撃者に先回りして対処できる力を与えます。

Dellの包括的なMITMソリューションでビジネスを保護し、顧客の信頼を維持して、将来を見据えた運用を実現しましょう。今すぐお問い合わせください。レジリエンスと安全性の高いビジネスの未来に向けて取り組みましょう。

デル・テクノロジーズと提携することで、サイバー脅威に対して積極的に取り組み、顧客やステークホルダーとの永続的な信頼関係を築いて、安全性が失われつつあるデジタル世界で事業を成功に導くことができます。より安全な未来は、Dellから始まります。

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