DELL Technologies

DDoS：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

DDoS攻撃の脅威の増大

分散型サービス拒否(DDoS)攻撃は、デジタル時代において最も広範囲にわたる破壊的な脅威の1つとなっています。侵害されたデバイスが属する膨大なネットワークを利用するDDoS攻撃は、標的となるシステム、サーバー、ネットワークに大量のトラフィックを送りつけます。この絶え間ないトラフィックの急増により、業務に遅延が生じたり、業務が停止したりします。そして多くの場合、その過程でビジネスが損害を被ります。

スタートアップ企業から多国籍企業にいたるまで、増大するDDoS攻撃の脅威の影響を受けない組織は存在しません。企業がデジタル インフラストラクチャにますます依存するようになるなか、この攻撃は経済的損失から評判の低下まで、壊滅的な影響をもたらします。デル・テクノロジーズはこの課題の重大性を認識しており、企業が防御を強化し、困難を切り抜けるのに役立つ、拡張性のある革新的なソリューションを提供しています。

DDoS攻撃とは

DDoS攻撃は、ネットワーク、サービス、サーバーの通常の機能を停止させることを目的に、複数のソースから大量のトラフィックを送りつけるサイバー攻撃です。この攻撃はボットネットを悪用して実行されます。ボットネットとは、感染したデバイスで構成されるネットワークであり、攻撃者は感染デバイスを遠隔操作で制御します。

DDoS攻撃の攻撃方法

1. **ボットネットの採用：**サイバー犯罪者は、数千台または数百万台のデバイスにマルウェアを感染させ、事業運営を不能にする攻撃に利用できるボットネットを形成します。
2. **トラフィック フラッディング：**攻撃者が、ボットネットに大量のリクエストをターゲット サーバーに送信するよう指示します。これによりシステムの処理速度の低下やクラッシュを引き起こし、また正規ユーザーがシステムを使用できなくなります。
3. **システムのオーバーロード：**システムに大量の不正なトラフィックが送られると、そのシステムは正当なリクエストに対応できなくなり、サービスの停止や重大な遅延が発生します。

一般的な手法

- **ボリューム型攻撃：**大量のトラフィックでネットワークの帯域幅を使い果たします。
- **プロトコル攻撃：**TCP/IPなどのプロトコルの脆弱性を悪用してリソースを消費します。
- **アプリケーション層攻撃：**Webサイトやデータベースなどの特定のアプリケーションを標的にして、機能を中断させます。

これらの攻撃は絶えず進化しており、事業を保護しようとする企業にとって厄介な問題となっています。

ビジネスへの影響

財務的な影響

1回のDDoS攻撃で、収益の損失、ダウンタイム、リカバリー費用を含めて数百万ドルの損失が発生する可能性があります。eコマース プラットフォームや金融サービスなどのリアルタイム トランザクションに頼っている企業は、サービスが数分利用できなくなっただけでも大きな影響を受ける可能性があります。

業務の中断

DDoS攻撃による中断により、生産性が低下し、重要なプロセスに遅れが発生して、重要なサービスへのアクセスが妨げられます。医療や製造などの業界では、運用上のダウンタイムの影響が広範囲に及ぶ可能性があります。

評判へのダメージ

顧客やクライアントがサービスの中断を経験すると、信用が低下します。インシデントが長時間続いたり、繰り返し発生したりすると、企業の評判が長期的に損なわれ、顧客離れにつながり、市場での信用が低下する可能性があります。

実例

2020年に大手金融機関が継続的なDDoS攻撃を受け、オンライン バンキング サービスが数時間停止しました。直接的な収益損失と評判の低下により、損害額は**5,000万ドル**を超えました。

警戒すべき統計

Zayo GroupのDDoS Insights Report（2024年2月）によると、2023年の保護対策が取られていない組織の1分あたりの平均損失額は**6,000ドル**、インシデントあたりの平均損失額は**408,000ドル**にのぼりました。しかも、このような攻撃の発生頻度は増加しており、**年間1,000万件を超える攻撃が報告されています**。これらの統計は、堅牢な予防メカニズムの差し迫った必要性を示しています。

2,050万件

2025年第1四半期に阻止されたDDoS攻撃の件数

出典：CloudflareのDDoS脅威レポート（2024年）

デル・テクノロジーズでDDoS攻撃に対処

デル・テクノロジーズは、企業がDDoS攻撃を未然に防ぎ、検出し、復旧できるよう支援する高度なソリューションを提供しています。

Dell Trusted Deviceでエンドポイントを強化

エンドポイントは、DDoS関連の脅威の重要な侵入経路です。Dell Trusted Deviceは、セキュアBIOSやSafeIDなどハードウェア組み込みの堅牢なセキュリティ機能を備えています。このようなセキュリティ機能により、不正アクセスを防ぎ、システムの整合性を維持します。

サーバーのセキュリティ

DellのサーバーソリューションはDell Trusted Serverテクノロジーなどの組み込み型セキュリティ対策を備えています。これには次の機能が含まれます。

- **ハードウェア ルート オブ トラスト：**この機能により、サーバーのハードウェア コンポーネントが起動時に検証されます。これにより、改ざんや不正な変更に対処するセキュリティの基盤が実現します。
- **組み込み型のセキュリティ機能：**Dellサーバーは自己暗号化ドライブとエンドツーエンドのブート検証を備えています。これにより、不正アクセスを防止し、データの整合性を確保します。
- **サイバー レジリエンス：**このアプローチには、異常、侵害、不正な操作を検出する機能が含まれており、組織はサイバー インシデントから迅速に復旧できます。
- **包括的なデータ保護：**DellのTrusted Serverソリューションは、静止時と転送時のデータを保護する統合セキュリティ メカニズムを備えています。これには事業の継続性を確保するための高度な暗号化技術と自動リカバリー オプションが含まれています。

これらの機能により、サーバーは運用の安定性を維持しながら、トラフィックの急増に耐えることができます。
ストレージ ソリューションは、攻撃発生時に重要なデータの可用性と整合性を保護し、中断を最小限に抑えます。

ストレージ セキュリティ

Dell Storageは、脆弱性を最小限に抑え、脅威を早期に検出して、攻撃が発生した場合に迅速に復旧できるよう設計されているさまざまな統合セキュリティ対策と高度なテクノロジーによって、DDoS攻撃の防止を支援します。主な手法は次のとおりです。

- **プロアクティブな脅威検出：** Dellのストレージ ソリューションは、インテリジェントなモニタリングとAIを活用した異常検出を採用。DDoS攻撃を示している可能性がある異常なアクセス パターンを特定します。これらのツールはリアルタイムのセキュリティ インサイトを提供し、自動化された脅威対応をトリガーして攻撃の影響を軽減できます。
- **ルート オブ トラスト アーキテクチャ：** ストレージ コントローラーに統合されたこのアーキテクチャにより、ファームウェアの信頼性が確保され、不正な変更が防止されます。これによりストレージ ハードウェアのセキュリティが強化され、DDoS攻撃時に侵害が発生する可能性が低減されます。
- **多要素認証(MFA)とアクセス制御：** MFAとロールベースのアクセス制御(RBAC)を実装することで、ストレージ システムへの不正アクセスを防止し、DDoS攻撃に関連する脅威に対する保護が強化されます。
- **マイクロセグメンテーションとネットワーク分離：** Dellは、ストレージ システムを分離し、ワークロード間のアクセスを制限することで、潜在的な攻撃ベクトルを最小限に抑え、侵害が発生した場合にストレージ システムをラテラル ムーブメントから保護します。
- **安全なスナップショットと不変ログ：** Dellのストレージ ソリューションは安全なスナップショットと不変ログを備えており、データの整合性を確保し、DDoS攻撃からの迅速なリカバリーを支援します。これらの機能により、フォレンジック分析とインシデント調査が容易になり、ITチームでは攻撃ベクトルの検出と分析が行えるようになります。
- **Cyber Recoveryヴォールト：** Dell PowerMaxやPowerProtect Cyber Recoveryヴォールトなどのソリューションは、不変的なエアギャップ型バックアップを作成し、ランサムウェアなどの攻撃を防ぎます。これらのバックアップをリストアすることで、再感染のリスクなしに事業を継続できます。

Dell Storageとサイバー レジリエンスは、これらの包括的なセキュリティ機能とテクノロジーを統合することで、組織がDDoS攻撃を効果的に防止し、レジリエンスと安全なIT環境を維持できるようにします。

CrowdStrikeによるプロアクティブなモニタリング

状況が悪化する前に異常なトラフィック パターンを検出するには、リアルタイムのモニタリングと高度な分析が不可欠です。CrowdStrikeは、Dellのエコシステムに組み込まれ、行動分析とAIを活用したインサイトを使用することで、正当なアクティビティーを攻撃トラフィックと区別し、迅速な修復を可能にします。

Dell PowerProtectでデータの整合性を維持

Dell PowerProtectは、DDoS攻撃の発生中でも重要なデータの安全性を確保し、このデータにアクセスできるようにします。不変バックアップ機能と分離されたリカバリー環境により、インシデント発生後にシステムをリカバリーして、ダウンタイムを最小限に抑えることができます。

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。

実際の導入事例

先日、あるグローバルなeコマース プラットフォームが、DellのPowerProtectソリューションとプロアクティブな検出機能を活用して、高度なDDoS攻撃を阻止しました。重要なシステムを分離し、緊急リカバリー プロセスを導入することで、記録的な速さで完全な業務を再開し、経済的損失を軽減し、クライアントからの信頼を維持できました。

多層型セキュリティ アプローチ

DDoS攻撃に対する防御に成功するには、多層化された適応型の防御が必要です。Dellは、そのテクノロジー製品を補完するため、次の戦略を推進しています。

防御を強化するための重要なステップ

- **ゼロトラスト アーキテクチャ：**「決して信頼せず、常に検証する」モデルを実装して、各ユーザーとデバイスを精査します。
- **高度な暗号化：**すべての層にわたって通信を暗号化し、攻撃に発展する可能性がある試行中に送信される機密データを保護します。
- **従業員トレーニング：**不注意による侵害を防ぐため、疑わしいアクティビティーの特定と安全なプロトコルの遵守に関して従業員を教育します。
- **定期的なシステム テスト：**大量のトラフィックに対するシステムの準備状況を評価するため、侵入テストや負荷テストなどの定期的な評価を実施します。

これらのアクションをデル・テクノロジーズソリューションと組み合わせることで、高度な脅威に対する堅牢な防御メカニズムが構築されます。

サイバーセキュリティを強化するパートナーシップ

デル・テクノロジーズは、**Microsoft**、**CrowdStrike**、**Secureworks**などの業界大手企業と連携して、その機能を強化しています。これらのパートナーシップにより、最高の脅威インテリジェンスと高度な検出方法がDellの包括的なフレームワークに組み込まれ、保護が強化されます。

Dell Professional Servicesを活用

DellのProfessional Servicesは、テクノロジーだけでなく、DDoSの課題に直面している企業に専門的なガイダンスを提供します。Dellのチームが、インシデント対応からカスタマイズされたセキュリティ アーキテクチャに関するコンサルティングにいたるまで、組織が迅速に復旧し、将来的な防御を強化できるようにするためのサポートを提供します。

より良い未来を築くために

デル・テクノロジーズは、単なるテクノロジー プロバイダーではありません。お客様のパートナーとして、進化するDDoS攻撃の脅威からビジネスを守ることに尽力します。Dellは、最先端のテクノロジー、深いパートナーシップ、実用的なインサイトを組み合わせることで、事業運営を保護し、クライアントからの信頼を維持し、積極的に成長を追求できるよう企業を支援します。

今すぐレジリエンスへの第一歩を踏み出しましょう。デル・テクノロジーズにご相談ください。DDoSの脅威からビジネスを守り、未来を安全に守るためのセキュリティ対策をご提案します。

デル・テクノロジーズは、DDoSサイバーセキュリティの課題を克服できるよう企業を強化し、相互につながり合う世界で成功を収めるための鍵は安全な基盤であるということを証明しています。

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

の詳細はこちら
Dellのソリューション

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