DELL Technologies

サイバーセキュリティ対策ガイド：

最新のサイバー脅威に対応する方法

デジタル世界は今や、どこに危険が潜んでいるかわからない荒野です。1回のクリック、ダウンロード、ログインが、巧妙に仕込まれたサイバー トラップを踏んでしまう可能性があります。

今日のサイバー ランドスケープは、ランサムウェア、DDoS攻撃、フィッシング詐欺、バックアップへの侵入といった脅威がますます高度化しており、かつてないほど危険性が高まっています。ハッカーはAIを活用して従来の防御の裏をかきます。かつては日和見的だったその攻撃は、広範な被害を与え得る計算ずくの執拗な脅威へと姿を変えました。

Dellのお客様からは、ハッカーがソーシャル メディアをスクレイピングし、サイバーセキュリティ意識が最も高い従業員さえも欺くような説得力のあるメッセージを作成する、AIを活用した攻撃が報告されています。

こうした事例は、攻撃者が高度なテクノロジーを悪用して、前例のない緻密さで組織を操作し、欺き、侵入していることを痛感させるものです。

このような過酷な環境を生き抜くには、最先端のツール、プロアクティブな戦略、警戒の文化を組み合わせた、包括的なサイバーセキュリティ戦略が必要です。本ガイドでは、今日のサイバー脅威に対するレジリエンスを高めていただけるよう、こうした戦略の構成要素について検証します。

組織を守るための道標：ゼロトラスト フレームワーク

AI主導の脅威が広がる今日、ゼロトラスト フレームワークの採用はもはや任意ではありません。攻撃者は、偵察の自動化、認証情報の盗み出し、攻撃手法の迅速な適応にAIを使用しているため、従来の防御は効果を失いつつあります。ゼロトラストは、「侵害はあるもの」という考え方に立った運用方法です。すべてのアクセス要求を継続的に検証し、厳格な認証プロセスを実装して、リスクを最小限に抑えます。

ゼロトラストは、ユーザー、デバイス、アプリケーションをプロアクティブに監視することで、不正アクセスやデータ侵害が起きる可能性を減らします。これは、ID管理に対する最新の包括的なアプローチです。

現場の保護：攻撃対象領域の縮小

AI主導の脅威を防ぐには、攻撃対象領域を縮小することが不可欠です。攻撃者はエンドポイント、API、サプライ チェーンの脆弱性をしばしば悪用します。エンドポイントとAPIはネットワークへのエントリー ポイントとして機能し、マルウェアの展開や機密データの窃取を目的とした攻撃の標的になることがよくあります。

こうした領域を保護するには、強力な認証、転送中のデータの暗号化、定期的な脆弱性テスト、エンドポイントでの検出および対応(EDR)ツール、パッチ管理、デバイスの強化など、多層的な防御戦略が必要です。エンドポイント監視ソリューションと継続的な脅威検出により、悪意のあるアクティビティーをリアルタイムで特定して阻止できます。

組織が自社のソフトウェア サプライ チェーンと開発ライフサイクルを保護するには、プロアクティブな戦略を採用する必要があります。アクセス権限を最小限にすれば、許可されたユーザーとアプリケーションのみに重要なシステムとのやりとりを制限できますし、脅威の検出と対応を自動化すれば、脆弱性が発生した場合に迅速に対処できます。

巧妙な攻撃の追跡：プロアクティブな脅威検出と対応

AIを活用した攻撃は、脆弱性を突き、正当な動作を模倣し、動的に適応してセキュリティ対策を回避するため、検出が困難です。こうした巧みな脅威には、事後対応策だけでは不十分です。高度な脅威検出システムと迅速な対応機能を組み合わせる必要があります。AIと機械学習を活用することで、セキュリティ チームは行動パターンを分析し、異常を検出し、リアルタイムで脅威に対応できるため、重大な損害が発生する前に問題に対処できます。

効果的な検出および対応システムでは、リスクを特定して自動化された対応をトリガーできるように、膨大な運用データを収集する必要があります。この脅威インテリジェンスも自己強化型であるため、システムがさらにスマートになり、新たな攻撃手法をプロアクティブに特定して対処できます。

DELL Technologies

未然防止の徹底：インシデント対応とリカバリー

まずは攻撃を防ぐことが先決ですが、攻撃は避けられないという前提で行動する必要があります。目標は、最小限の損害で攻撃を切り抜けることです。効果的な戦略には次の2つの要素が含まれます。

- 強力なインシデント対応およびリカバリー(IRR)計画。
- 重要なデータとアプリケーションのバックアップを中心としたテクノロジー面での対策。

インシデント リカバリー計画は包括的でなければなりません。強力なサイバー攻撃によって会社のほぼすべての業務が停止する可能性があるため、インシデント リカバリー計画では、サイバー インシデント発生時に会社のすべての部署が取るべき行動を網羅する必要があります。また、コミュニケーション テンプレートをあらかじめ作成し、対社内・対社外それぞれの情報伝達方法についても決めておかなければなりません。同様に、計画を定期的に更新し、維持することも必要です。結局のところ、計画の有効性は実践演習の頻度次第です。攻撃が発生した場合に、誰もがとっさに行動できるようにしておく必要があります。

テクノロジーの観点からは、まず、必要最低限の企業体制(MVC)を決定すべきです。つまり、紙と鉛筆で作業することになっても稼働させ続けるべきシステムはどれか、セールス機能の継続は不可欠か、カスタマー サービス機能はどうか、などを判断する必要があります。

こうしたことが決まったら、それらに基づきバックアップとリカバリーのメカニズムを構築します。既知の正常なデータに戻す能力を備えておくと、迅速に業務を再開できるだけでなく、データを人質に取ろうとする悪意のある攻撃者の力を削ぐことにもなります。さらに、最新のIR戦略では、従来のアプローチと異なり、チャットボットや仮想エージェントなどのAI/LLMシステムをTier 1資産として扱い、決済システムや顧客データと同じ優先度でリカバリーする必要があります。

高度な脅威に対抗するため、IR計画では自動化と手動チェックのバランスを取る必要があります。全システムのアウテージが発生した場合に組織がどのように機能するかを把握することは、極めて重要です。ペンと紙に戻さなければならなくなった場合は、どうなるでしょうか。

全員協力体制の構築：従業員の意識向上

従業員は、サイバー脅威に対する最初の防衛線です。危険な荒野を進むサバイバル チームのように、メンバー全員がリスクの特定とリソースの保護において重要な役割を果たします。この防御を強化するには、高度なフィッシングやディープフェイクといったAI固有の脅威を含む攻撃シミュレーションなど、効果実証済みの意識向上プログラムが必要です。

最良のプログラムは、継続的な教育、オープンなコミュニケーション、現実世界でのシミュレーション、責任を共有する文化を組み合わせたものです。現場スタッフから経営陣まで、全員が従来の脅威とAI主導の脅威の両方を理解したとき、十分な知識と警戒心を併せ持つ、団結した組織が完成します。チームワークと準備を促進することで、組織は進化するサイバー リスクに先手を打ち、潜在的な攻撃に対するレジリエントな防御体制を構築できます。

AI主導の攻撃に対してレジリエンスを維持するためのベスト プラクティス

AI主導の攻撃に対するレジリエンスを維持するには、プロアクティブで戦略的なアプローチを採用する必要があります。10のベスト プラクティスをご紹介します。

ゼロトラスト アーキテクチャ

継続的な検証、厳格なアクセス制御、ネットワーク セグメンテーションを要求し、あらゆるユーザーとデバイスに対してアクセス許可前の認証を行うことで、急速に変化するAI主導の攻撃を阻止して封じ込めます。

IDおよびアクセス管理の強化：

堅牢な認証（MFA、RBAC）を導入し、強力な認証情報ポリシーを適用して、フィッシングや認証情報スタッフィングの成功率を下げます。

資産検出とインベントリーの自動化：

クラウド、IoT、シャドーITを含むすべての資産を継続的に検出して監視し、隠れたリスクを回避します。

マイクロセグメンテーションとネットワーク アクセス制御：

ネットワークとワークロードをセグメント化して分離し、攻撃者の横方向の移動を阻止して脅威を封じ込めます。

エンドポイントとAPIの強化：

高度なエンドポイント保護(EDR/XDR)と安全なAPIゲートウェイを使用します。強力な認証、レート制限、入力検証、暗号化を行います。

脆弱性とパッチの厳格な管理：

OS、ファームウェア、アプリケーション、API、サードパーティー製ソフトウェアのスキャンと迅速なパッチ適用を自動化します。

AI主導の脅威の検出と監視：

行動検出と異常検出にAI/MLを活用し、捉えにくい脅威や自動化された脅威をリアルタイムで検出します。

インシデント対応の自動化：

自動プレイブックを使用した、脅威の迅速な隔離、封じ込め、修復により、攻撃者の滞留時間を最小限に抑えます。

定期的なリアル シミュレーションと継続的な改善：

机上演習に加えてレッド チーミングやフィッシングのシミュレーションを実施し、結果に基づきIR計画と検出モデルをアップデートします。

変えることができない、エアギャップ型のバックアップとリカバリー：

耐タンパー性が高いバックアップ（エアギャップ型、定期的なテストが理想）を保管し、クリーンで迅速なリカバリーを可能にします。

DELL Technologies

デル・テクノロジーズ：未知の領域に踏み込むための案内役

高度なサイバー脅威から組織を守るには、進化するリスクに先手を打つための適切なツールと専門知識が必要です。今日の複雑なサイバーセキュリティ ランドスケープでデータ、システム、評判を守るには、強固な戦略が欠かせません。デル・テクノロジーズは、あらゆる規模の組織のニーズに対応する包括的なソリューションを提供しています。

Dellは、安全なサプライ チェーン、高度な脅威の検出、エンドポイント保護から、安全なデータ管理まで、最新のサイバー攻撃防御に必要なテクノロジーを通じて、お客様のビジネスを守ります。業界をリードする専門技術に裏打ちされたDellのチームが、お客様と緊密に連携してカスタム セキュリティ戦略を策定します。Dellは、リアルタイムの監視、自動化された脅威対応、ゼロトラスト アーキテクチャなどの機能で、組織が常に先を見据え、レジリエンスを維持できるよう支援します。

ランサムウェア、フィッシング攻撃、法令遵守のいずれに取り組む場合でも、お客様が今日の脅威ランドスケープを自信をもって進んでいけるようサポートします。デル・テクノロジーズと提携して、ビジネスを守り、デジタル時代に成功を収めましょう。事業運営に安全性と効率性を確保して、あらゆる変化に備えましょう。

> 攻撃中はシステムがアクセス不能になる可能性があるため、インシデント対応計画は紙に印刷する必要があります」
>
> ***Rachel Tyler***
> *Dell Services*、サイバーセキュリティ アドバイザリー コンサルタント

有効なDellの製品とソリューション

注目のDellソリューション	説明
Dell Trusted Infrastructure	Dellのサーバー、ネットワーキング、ストレージ、サイバー レジリエンスを組み合わせたソリューション。最新かつ安全で耐障害性の高い基盤を一体となって構築し、イノベーションを起こします。
サイバー レジリエンス	データの保護と安全なリカバリーを目的とする、包括的なソリューション ポートフォリオ。アプライアンス、ソフトウェア、アズ ア サービス製品が含まれます。
サイバーセキュリティ サービス	ワークロード全体にわたる包括的なセキュリティ戦略の策定と実装を支援する、サービス一式。アドバイザリー サービス、vCISO、Managed Detection and Response、侵入テストと脆弱性テスト、インシデント対応とリカバリーが含まれます。
Dell Trusted Workspace (Endpoint Security)	組み込み機能とオプションのアドオン機能の組み合わせ。ビジネス向けPCを保護するように設計されています。安全なサプライチェーン プラクティスに基づいて構築された組み込み機能には、SafeBIOSとTPMを使用したSafeIDが含まれます。オプションのアドオンには、Secured Component Verification、ControlVaultを使用したSafeID、パートナー ソフトウェアのCrowdStrikeとAbsoluteなどがあり、ワークスペースのセキュリティを最大限に高められます。

dell.com/cybersecuritymonth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