



IDなど認証情報侵害への迅速な対応

課題

データセキュリティに関する従業員の能力を高める

従業員のリスクは加速度的に高まっています。企業はウェブやクラウド上の脅威からデジタルフットプリントを守るため、組織文化の一環として最新のセキュリティ意識向上ソリューションに投資しています。従業員レベルでは、クリックしてしまいそうなファイルが添付されたフィッシングメール、クローン化されたウェブサイト、偽のソーシャル投稿、インスタントメッセージの招待に含まれる高リスクの脅威を特定し、理解することが優先されます。

フィッシング、ソーシャルエンジニアリング、悪意のある添付ファイルは、企業に高いリスクをもたらします。このような事象に対処するための正しい知識を従業員に教育すること（たとえば、悪意があるかもしれないメールは直ちに適切に報告する）は、サイバーリスクを減らすための第一歩です。しかし、どれだけ予防措置を講じても、100%防御できるわけではありません。ITチームには、自社のユーザーの利便性を損なうことなく、読み込まれたページを検査し、脅威となるものが含まれていないか、すべての添付ファイルをスキャンする最新のテクノロジーが必要です。

増加するフィッシング攻撃

ソーシャルエンジニアリングや人工知能 (AI) の進歩により、いまやフィッシングメールは本物と見間違ふほどになっています。その手口は一層パーソナライズされ、経営幹部やそのアシスタント、取締役、管理職に加え、IT、法務、人事、パートナーチャネル部門のスタッフなど、組織全体の特定の個人を標的にします。主な目的は、疑うことを知らない従業員を信じ込ませて、機密情報を漏えいさせたり、マルウェアをインストールさせたりすることです。

最も単純でありながら最も効果的なフィッシングメール攻撃には、従業員をウェブページに誘導し、個人の認証情報 (ID、ユーザー名、パスワード) やクレジットカード番号を入力させるリンクを含む悪意のあるメッセージが含まれます。このようなサイバー攻撃は巧妙に調整され、提示され、複数の段階を経て実行されます。これによって、大量のデータやプライバシーの侵害、デバイスやシステムへの感染、ひいては攻撃者からのランサムウェアによる損害を引き起こす可能性があります。



フィッシング攻撃プロセス

ITセキュリティリスク

フィッシング攻撃の目的は、機密情報またはインフラにアクセスすることです。攻撃者は、標的がたとえ低い権限しか持たない個人であったとしても、従業員をだましてマルウェアや内部フィッシング攻撃を起動させることで高い権限を取得することにより、次の攻撃を実行するための扉を開くこととなります。内部フィッシングは、危険にさらされているユーザーと他者との信頼関係を活用するため、攻撃者にとって魅力的です。メールゲートウェアを使用してメールをスキャンするだけの従来型のアプローチは、内部のすべてのメールトラフィックをバイパスしてしまうため、社内の脅威の検知には効果がありません。

従業員がマーケティングメールとフィッシングメールを正確に区別できず、かつITチームがメールの脅威を確認し、確実にフィルタリングすることができないとき、ITセキュリティのリスクは増大します。このようなリスクを軽減するには、メールトラフィックを総合的に追跡し、悪意のある行為をリアルタイムで阻止するルールを備えた多層的なメールセキュリティのアプローチが必要です。

継続中の企業活動をサポートするため、ITチームはバランスの取れたアプローチを浸透させる必要があります。あまりにも制限の多い許容可能な利用ポリシー (AUP=Acceptable Use Policy) は生産性を阻害します。その代わりに、通信が「内部」からのものなのか、それとも「外部」からのものなのかを従業員に知らせる通知を受信メールの先頭に埋め込むことによって、生産性を制限せずに意識を高めることができます。このアプローチでは、従業員とビジネスのニーズに柔軟に対応し、従業員のセキュリティ意識向上およびトレーニング・イニシアチブの一環として効果的なコミュニケーションを確保するために、ゼロトラストによるITセキュリティ運用とアクセス・ポリシー管理を施行し、更に常に見直す必要があります。

機能

堅牢なセキュリティでビジネスアプローチを先鋭化

その目的は、サイバー脅威からビジネスを守りながら、ビジネスを成功させることです。これには、さまざまなデジタル通信 (メール、ウェブブラウジング、インターネットを介してアクセスされるアプリケーションなど) を通じて従業員情報を保護することが含まれます。しかし、企業が成長し、組織の脅威の対象領域 (アタックサーフェイス) が広がるにつれて (たとえば、在宅勤務の増加)、この目的の達成はますます難しくなります。そのため、統一されたポリシーと簡素化された管理による多層的なセキュリティ対策が不可欠です。労働慣行の発展と変化に加えて、メールによるフィッシングやウェブ脅威の複雑化によって、インターネット上の脅威に対するソリューションは従来のセキュリティ運用アプローチからゼロトラストのような高度なアーキテクチャに移行しています。この最新のアプローチを適用することによって、企業は従業員とITに対するセキュリティリスクを下げ、アクセス管理を絶えず評価し、トラフィックの状況を見抜き、権限を設定し、意識を高めることができます。

事前予防につながる脅威検知へ

統合サイバーセキュリティプラットフォームであるTrend Vision Oneは、プロアクティブなセキュリティ測定と制御を導入することで、インシデントの発生前および発生後のアクションを検出、フィルタリング、追跡、阻止することができます。これは、弊社のメールゲートウェイ、クラウドアプリケーションアクセス制御およびセキュアウェブゲートウェイ (SWG) 機能を活用し、従業員に対する戦略的なセキュリティ意識向上とトレーニング戦略をサポートすることで実現されます。ITの有効性は下記のツール、機能およびベストプラクティスの支援によって達成することができます。

- **可視化と制御:** セキュアウェブゲートウェイ (SWG) およびクラウドアクセスセキュリティブローカー (CASB) を活用することにより、すべてのウェブトラフィック、ウェブアプリケーションの使用状況の詳細 (保存されたファイル、送信されたメールを含む) を表示します。
- **パフォーマンス:** 強力なクラウドインフラストラクチャ上のグローバルPoP (Point of Presence=ネット接続するなどに利用する最寄りの接続点) は、SSLトラフィックの検査速度、ダウンロード時のマルウェアのスキャン速度およびデータ損失防止 (DLP) 違反の認識速度を高め、遅延時間を最小限に抑えます。
- **俊敏性および拡張性:** 弊社のクラウドネイティブ型ウェブゲートウェイテクノロジーにより、従来のオンプレミス型ウェブゲートウェイよりも高速に、しかもダウンタイムなしで拡張することができます。これによって、セキュリティ、可視性、管理を犠牲にすることなく、大きな仮想イベントを処理したり、在宅勤務への対応をサポートしたりすることができます。
- **多層防御:** 弊社の統合機能は、送信者のコンテンツや画像の解析、機械学習などの複数の技術を用いて、フィッシング、スパムおよび潜在的に危険なメッセージに対する多層的な保護を送信中および静止時に提供します。

境界を越える

Trend Vision One™のレンズを通して実績のあるテクノロジーを活用することで、メールゲートウェイ、クラウドアプリケーションへのアクセス制御、SWGの機能だけでなく、より広範なエコシステムが追加データを提供できるようになります。これにより、侵害されたアカウントの特定、自動化されたアクセスの意思決定、豊富な遠隔測定、レポートの可視化、API統合が可能になり、シンプルで一貫性のあるポリシー制御が実現します。

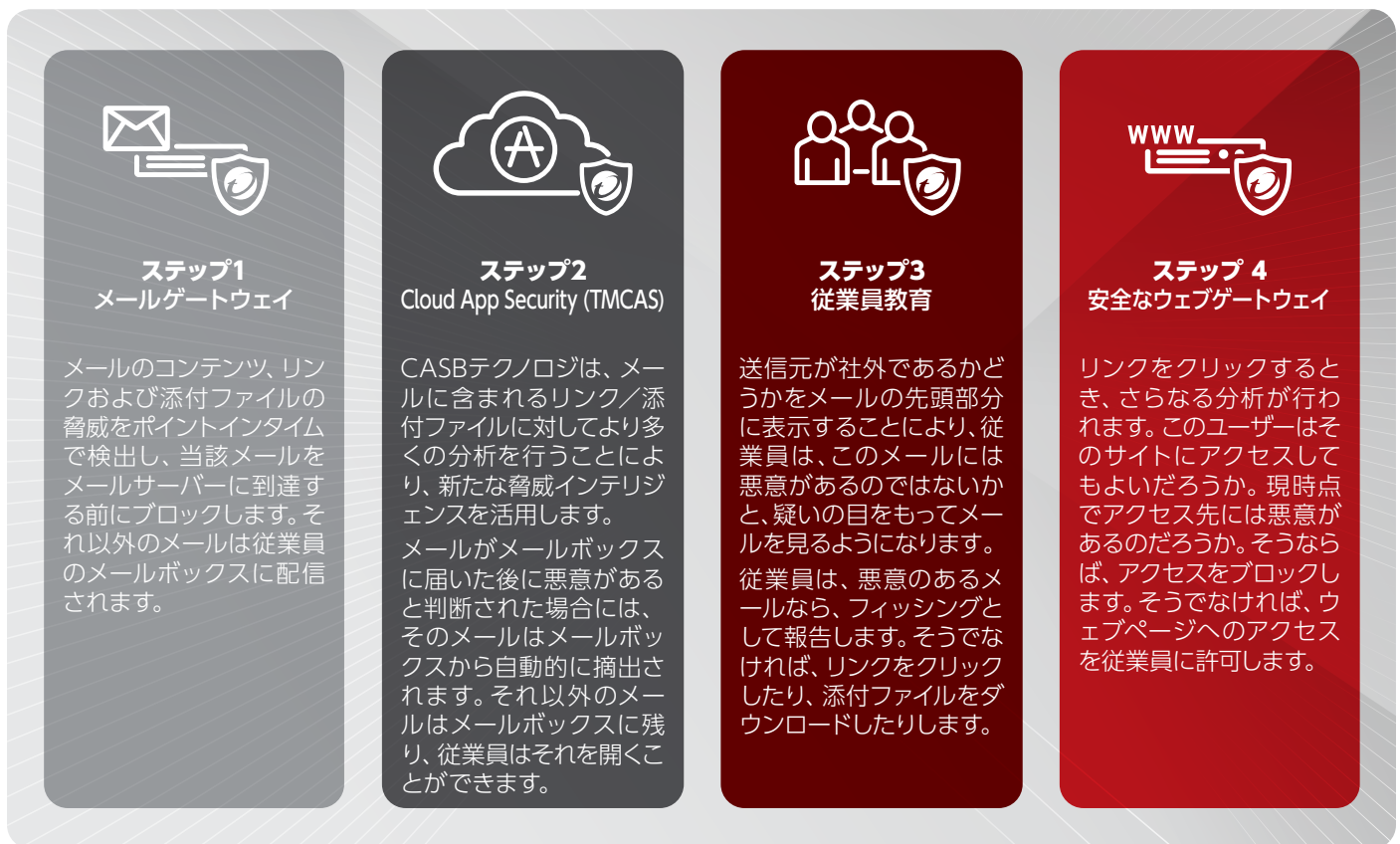
実装

ゲートウェイおよびセキュリティのソリューション

受信メッセージについては、メールゲートウェイを介した迅速な検査が必要です。まず、**Trend Micro™ Email Security (TMEms)** が、ビジネスメール詐欺 (BEC)、コンテンツに基づく潜在的フィッシング攻撃、既知の悪意あるリンクおよびファイルに由来する脅威をメールサーバに到達する前に検出します。TMEmsはMicrosoft Exchange、Microsoft 365、Gmail™、その他のホスト型またはオンプレミス型のメールソリューションを保護します。

次に、メールサービス/メールサーバに送られたメールは、**Trend Micro™ Cloud App Security (TMCAS)** によりもう一度評価されます。メールを「静止状態」でスキャンすることで、メールの配信に影響を与えずに、さらに徹底的なスキャンを行うことができます。また、過去に遡って対応することが可能なため、新たなインテリジェンスを受け取ったときに、悪意のあるメールを隔離や削除することもできます。更にこのTMCASは、組織内のメールもスキャンできるため、漏えいしたアカウントが他の従業員をフィッシングすることも防ぐことができます。

弊社のクラウドベースのSWGを「クリック時点」で使用することにより、**Trend Micro™ Zero Trust Secure Access** がアプリケーションレベルでウェブおよびインターネットトラフィックのフィルタリングを行います。これには、アクセス先またはダウンロードしようとするファイルに悪意があるかどうかの評価も含まれます。許容可能な利用ポリシー (AUP=Acceptable Use Policy) を適切に使用することで、正式に許可されていないアプリケーションへのアクセスが制限され、従業員が機密情報を入力するのを防止することができます。SWGはエンドユーザーとインターネットの間に介在し、TLS/SSLを含む複数のセキュリティ技術を用いてインラインでトラフィックを検査します。



フィッシングメールを検出・分析・停止する手順

次のステップ

異なるセキュリティ・コア技術を多層的に実装することによって、組織は取り組みを先鋭化し、従業員のデジタルフットプリントの増大に応じた適切なレベルの保護を提供することができます。Trend Microは以下の無料トライアルをご用意しています。最も一般的な形態のサイバーリスクを軽減したい場合には、統合型ソリューションをご利用ください。

[Trend Micro™ Email Security \(TMEms\) の30日間無料試用版](#)

[Trend Micro™ Cloud App Security \(TMCAS\)の30日間無料試用版](#)

[Trend Vision One \(Trend Micro™ Zero Trust Secure Access を含む\) テストドライブ](#)

©2023 by Trend Micro Incorporated. All rights reserved. Trend MicroならびにTrend Microのt-ballロゴおよびTrend Vision Oneは、トレンドマイクロ株式会社の商標または登録商標です。その他の各社の名称および製品名は、一般に各社の商標または登録商標です。本書に記載されている情報は、予告なしに変更されることがあります。[SB00_Vision_One_Use_Case_230309US]

収集される個人情報と理由については、当社ウェブサイト (trendmicro.com/privacy) のプライバシーポリシーに関する通知を参照してください。