E コマース E マガジン

Adastria、インターネットと安全に直接接続する環境を実現

Adastria は、日本と海外で 30 以上のブランドを展開し、およそ 1,400 店舗を運営するカジュアルファッションの小売企業です。

同社の成長戦略の中で、デジタル化は顧客体験と従業員体験を向上させる重要な推進力となっています。その一方で、ますます高度化するサイバー攻撃から顧客データを保護すること、そしてパートタイムの従業員が多く入れ替わりの激しい店舗での従業員へ適切なトレーニングを提供することが課題になっていました。

店舗には 1 台の PC が配置され、フロアでは多くの携帯デバイスとタブレットが使用されています。これらのデバイスのインターネットトラフィックは本社でセキュリティが管理されていますが、店舗にはインターネットに直接アクセスできるデバイスも存在します。

店舗の PC と携帯デバイスは、Web サイトの許可リストによりインターネットアクセスが厳しく制限されています。一方、店舗のタブレットと本社の PC はさまざまな Web サイトにアクセスしてファッショントレンドをチェックするため、制限の対象外です。

これらのデバイスは、フィッシングメールのリンクをクリックしたり、うっかり危険な Web サイトにアクセスしてマルウェアに感染したりなど、セキュリティ侵害の原因になる可能性があります。

Adastria の店舗と本社のすべてのデバイスは、エンドポイントのウイルス対策ソフトウェアがインストールされていますが、さらなる保護が必要とされました。

Adastria は、Akamai のクラウドベースセキュア Web ゲートウェイを選びました。Enterprise Threat Protector は、シンプルかつプロアクティブにすべての従業員を脅威から保護するソリューションです。

Akamai のセキュア Web ゲートウェイを導入した Adastria は、自社のデバイスとインターネット間の悪意のあるトラフィックを自動でプロアクティブに防止し、ランサムウェアなど重大なセキュリティインシデントのリスクを抑えることに成功しました。

「初期 PoC は、DNS サーバーからすべての DNS リクエストを Enterprise Threat Protector に送信するシンプルな構成をとりました。PoC から全社導入は、脅威検出を『アラート』から『ブロック』に変更するだけでした。すべてのデバイスの保護が 20 分の作業で完了しました」と、同社は述べています。

セキュリティとアクセス制御を備えた 1 つの製品
でユーザーとデバイスの安全を確保します：

Secure Internet
Access Enterprise

続きはこちら

API：すべての人々をつなぐアタックサーフェス

デジタル化が生活のあらゆる面で重要な役割を果たす中、Web アプリケーションのプログラミングインターフェース（API）は、今日のあらゆるデジタル体験の中核になっています。API は、さまざまなアプリケーションをつなぎ、データを迅速に取得するためのオープンな方法を提供します。

ところが、API の普及に伴い、API 攻撃のリスクも高まっています。この新たなアタックサーフェスが急速に拡大しているのです。Akamai のリサーチャーは、過去 1 年間の Web アプリケーションおよび API 攻撃を分析し、2022 年第 1 四半期の攻撃件数が**前年同期比で 3 倍**に達していることを確認しました。

この問題は拡大する一方です。従来のネットワーク・セキュリティ・ソリューションで API を保護している組織は、成功を収めていたとしても、まずまずの成果にとどまっています。旧式のネットワーク防御の基準では、その程度の効果しか得られないからです。ほとんどの場合、Web サイトや Web アプリケーションと同じリスクが API にも存在しますが、これらは別々に対応する必要があります。

この状況は、API を悪用した攻撃が最も頻度の高い攻撃ベクトルになり、エンタープライズアプリケーションのデータ侵害に発展するという Gartner 社の予測と一致しています。API は保護されていないことが多く、低コストで攻撃可能なため、Web API が攻撃者の主要ターゲットになっているようです。

ソフトウェア開発ライフサイクルの一部として DevOps を迅速に導入することも、プラットフォームの管理と統合における API の使用増加につながっています。GitHub のようなオープン・ソース・リポジトリで共有される API キーや機微な情報の公開が、深刻なリスクとなっています。ほとんどの開発者は、アプリケーションを構築する際に API セキュリティを考慮していません。企業には、すべてのパブリック API とプライベート API を保護するセキュリティ戦略の導入が不可欠となっています。

e コマース業界は最も攻撃を受けている業界の 1 つです。e コマース企業は API 主導のビジネスモデルを積極的に採用しており、攻撃に対する脆弱性が増しているため、これはある意味で当然です。

API セキュリティのベストプラクティスの詳細については、こちらをご覧ください：

API: The Attack Surface That Connects Us All

続きはこちら

Akamai は、ランサムウェアなどのラテラルムーブメント（横方向の移動）攻撃の拠点として使用される内部サーバーとなったコマンド・アンド・コントロール・サーバーで、大規模なデータ漏えいを確認したことがあります。

その他の重要な API の脆弱性には、弱点の多い認証とアカウントの乗っ取りがあります。API とは異なり、Web ブラウザは従来から、悪性ボットによる **Credential Stuffing 攻撃**に対する防御の最前線として、JavaScript をレンダリングし、captcha などのチャレンジを提示できます。

API は、JavaScript をレンダリングして Credential Stuffing 系の攻撃を防ぐといったことができません。この点が、盗んだ認証情報によるサーバーやエンドポイントへの不正アクセスを成功させる脆弱性を生み出しています。

API のアタックサーフェスを効果的に緩和するため、消費者向け小売企業は、プライベート API とパブリック API を保護できる適切なセキュリティ・ベストプラクティスを採用することが重要になります。

> *e コマース業界は最も攻撃を受けている業界の 1 つです。e コマース企業は API 主導のビジネスモデルを積極的に採用しており、攻撃に対する脆弱性が増しているため、これはある意味で当然です。*

API のセキュリティを確保するための 6 つのステップをご紹介します。

1. API の開発にセキュリティ重視のアプローチを採用します。開発者は、コード検査と API 検証を使用し、コーディングから実行までの間にセキュリティチェックを実施する必要があります。
2. すべての API を完全に可視化し、誰が、どこから、どのように API にアクセスしているかを把握できるセキュリティソリューションを導入します。
3. 顧客組織のニーズに合わせた事前対応型の API 保護を実現します。
4. API がデータを必要以上に公開しないようにします。API レベルでデータへのアクセスを強化します。機密データの共有を防止します。
5. Credential Stuffing やアカウントの乗っ取りを防ぐために、API に強力な認証と認可を採用します。
6. 内蔵されたボット緩和機能によって、Web アプリケーションと API の保護機能を展開します。

収益拡大のためのロイヤルティ

ロイヤルティは価値のある商品であり、ロイヤルティプログラムはもはや経費ではありません。

適切な（データ主導の）手法なら、ロイヤルティプログラムや顧客会員プログラムは、ビジネスの成長の促進剤になります。

しかし、多くの小売企業やブランドは、データの適切な活用がほぼできない基礎的なロイヤルティプログラムに固執しています。オンラインとオフラインの消費行動を組み合わせることは、特に苦手です。小売企業は、顧客を感情的に引き付ける適切な方法を見つける必要があり、そのためにはデータが必要なのです。

顧客には、小売企業がデータを悪用、紛失、誤用する心配はないと信頼してもらう必要があります。

最近、規制コンプライアンスが変更され、小売企業やブランドは、データの収集、保管、使用の正当性を説明し、透明化することを義務付けられました。これにより、消費者も自身のデータを保持する権利やデータ共有の意思に対する意識を高めています。

優れた小売企業は、より高度なロイヤルティ手法の使用を推進し、顧客関係を構築しています。このような企業は、ファーストパーティデータよりも、顧客の好み、つまり、体験に役立つデータに重点を置いています。たとえば、消費者が好む商品や、支払方法に関する情報を収集するのです。これにより、データ収集の理由が明確になります。

このようなターゲットを絞ったデータ収集と顧客とのやり取りには、2 つのメリットがあります。

第 1 に、小売企業は顧客データを使用して何か具体的な行動を取ることができます。第 2 に、共有されたトランザクションデータに基づいて新たなレベルのサービスや体験を提供でき、顧客をより引き付けられるようになります。

トランザクションデータを使用すると、ターゲットをより適切に絞り込め、傾向に基づいたセグメンテーションが可能になります。これは、数撃てば当たる式アプローチのセグメンテーションより、顧客に適切なものをタイミングよく提供できます。

それでも、ロイヤルティが基本的に信頼の対価であることを忘れてはいけません。率直に言えば、データを保護できないならば収集すべきではないのです。

弊社アカマイと、そのソリューションについてより詳しく知りたい場合は

ぜひお問合せください