Akamai お客様事例

金融会社が API を探索し、セキュリティを確保

銀行が、隠れた API を探索し、API リスクを評価して緩和し、規制要件を満たすことで、デジタルイニシアチブを保護

完全な可視化

セキュリティ体制の強化

デジタルイニシアチブのセキュリティの確保

金融サービス業界は、急速にデジタルトランスフォーメーションを受け入れ、進化し続ける市場で競争力を維持しています。人工知能やビッグデータ分析などのデジタル機能を使用することで、金融機関は革新的な商品を提供し、コストを削減し、よりパーソナライズされた効率的なサービスを顧客に提供することができます。

一方、デジタルトランスフォーメーションによってサイバー攻撃のリスクも高まります。このような拡大する問題に対処する上で、サイバーセキュリティはデジタルトランスフォーメーション戦略の重要な要素となっています。金融サービス企業は、自社のシステムを安全で耐障害性に優れたものにして、顧客のデータと資産を攻撃者から守る必要があります。

アジアのある大手商業銀行は、API セキュリティ体制を強化するために、Noname Security（現在は Akamai 傘下）に着目しました。API 侵害の勢いは驚異的です。Tech Wire Asia は、「現在、サイバーインシデントの 13 件に 1 件は API セキュリティの欠如に起因している可能性がある」と指摘しています。また、「API の脆弱性により、企業は年間で最大 750 億ドルのコストを負担している」と強調しています。

Akamai のお客様であるこの企業は、総資産 7,000 億ドル以上、法人顧客数 5,000 社以上であり、世界的に有名なウェルスマネジメントの評判を考慮すると、すべての API の脆弱性にできるだけ早く対処する必要がありました。

Financial Services

所在地

アジア

業種

金融サービス

ソリューション

Akamai API Security

Akamai

API とそのリスクを可視化する必要性

この金融機関ではすでに認証とトラフィック制御のための API 管理プラットフォームを展開していましたが、API の悪用とサイバー攻撃を防止する能力に疑問が生じていました。API ゲートウェイは必須かつ基本的な API セキュリティ制御を提供しますが、残念ながら API 特有の脅威から組織を適切に保護するためには不十分です。

たとえば、ゲートウェイはオブジェクトレベルの認可の不備（BOLA）を通常の API トラフィックとして認識します。API リクエストと応答の間の状況を認識する機能がないため、BOLA 攻撃は検知されずに通過し、重要なバックエンドサービスにアクセスできます。この欠陥により、組織は BOLA に対して脆弱なままになるだけでなく、他の攻撃やビジネスロジックの悪用が生じる可能性があります。

可視性の問題がもう 1 つあります。それは、正確な API インベントリーを維持できないことです。ほとんどの大規模組織と同様に、この銀行も自社環境内の未知の API に悩まされていました。現実として、エンタープライズは何千もの API を管理しており、その多くは API ゲートウェイなどのプロキシを介してルーティングされていません。このような API を「不正 API」または「ゾンビ API」と呼びます。これらの API は、おそらくは元従業員が展開したか、組織が API セキュリティを重視するようになる前に展開されたものです。理由の如何に関わらず、この銀行の API ゲートウェイはこれらの API を認識できなかったため、社内の API の実際の数を過小評価しやすくなっていました。

API セキュリティの課題に対応するために立ち上がる

この組織は、API 体制管理、ランタイム保護、テストのためのソリューションを含む完全な Noname API Security Platform（現在は Akamai API Security の一部）を自社環境全体に展開しました。その結果、同社のセキュリティ体制は大幅に改善し、世界で最も知られていない脅威ベクトルの脆弱性を検知して修復できるようになりました。

プラットフォーム内で未知の API を探索して明らかにすることができるようになり、完全な可視化とリスクの緩和が可能になりました。Akamai API Security は機微な情報を分類し、GDPR や HIPAA などの規制への準拠に役立つため、同銀行では API の乱立が大幅に減少し、コンプライアンスが向上しました。

また、同銀行は現在、リアルタイムで攻撃を阻止し、顧客データ資産を保護する能力も備えています。ランタイム保護ソリューションが API アクティビティを継続的に監視し、潜在的な脅威をインテリジェントに検知して優先度付けを行います。Akamai のプラットフォームは、Web アプリケーションファイアウォール、API ゲートウェイ、セキュリティ情報およびイベント管理、情報テクノロジーサービス管理、その他のワークフローツールと統合することで、手動、半自動、または自動で、脅威の修復を可能にします。

結果

API は瞬く間にハッカーが好む攻撃ベクトルとなりました。そして、攻撃の勢いが衰える兆候は見られません。たとえば、2022 年には「金融サービスに対する攻撃数が前年比で 257% 増加した」ことが報告されています。金融サービス企業は、Akamai API Security により、攻撃の被害者になることを回避し、このトレンドから身を守る態勢を整えることができます。特に、お客様のセキュリティチームは、API がもたらす危険をより深く理解し、より安全なシステムを構築することができます。

| 公開日：2024 年 8 月