2024 年の API セキュリティの影響に関する調査

小売および E コマース業界

同業者は API に対する脅威の増大をどのように認識し経験しているか

小売企業や E コマース企業のデジタルイニシアチブを支える API が攻撃を受けています。攻撃者は、ますます革新的な手法を使用して、保護が十分でない API からデータにアクセスして、クレジットカード情報を盗み、ロイヤルティプログラムから資金を吸い出し、Credential Stuffing 攻撃を仕掛けることができます。セキュリティチームはその影響を感じ、改善方法を模索しています。ただし、特に API のような別の攻撃ベクトルへの取り組みは、とてつもなく困難に思えるかもしれません。API の設定が誤っていたりビジネスロジックに欠陥があったりすれば、簡単に発見され、悪用される可能性があります。

なぜそう言えるのでしょうか。Akamai は、最高情報セキュリティ責任者（CISO）からアプリケーションセキュリティ（AppSec）のスタッフまで、1,200 人を超える IT およびセキュリティの専門家を対象に、API 関連の脅威に関する経験についての調査を行いました。

このレポートでは、当該の業界に関連する調査結果に的を絞っています。この業界では、回答者の 68% が、過去 12 か月間に API セキュリティインシデントが発生したと答えています。ではどのような影響があったのでしょうか？同業者の回答で最も多かったのは、チームのストレスレベルの上昇や、経営陣や取締役会からの信頼を損ねたというものでした。小売業および E コマースの専門家が、経験した API インシデントに対応するために 526,531 米ドルを費やしたと報告していることを考えると、この回答は理解できます。

業界の知見を得るには、詳細を「2024 年の API セキュリティの影響に関する調査」でご覧ください。

攻撃が増加、可視性は低下

小売および E コマース業界の回答者の大多数が API セキュリティのインシデントを経験しているものの、その 68% という平均値は、調査対象となった 8 つの業界全体で報告された 84% と比較して低くなっています。一方、業界同業者の今後 12 か月間の最優先のセキュリティ課題は、「生成 AI を活用した攻撃への防御」と「攻撃者からの API の保護」です。

API を優先することと攻撃の防止には関連があるのでしょうか。小売企業や E コマース企業のセキュリティチームは、API 保護の重要性を認識しており、その取り組みによってインシデントが削減される可能性はあります。しかし、当社調査では、これらのチームが API 悪用のすべての事例を把握しているわけではないことも示唆されています。

正規の API アクティビティと悪性または不正な API アクティビティを区別することは、小売企業や E コマース企業にとって依然として困難です。リスクの可視化も課題です。業界同業者の 67% が API の完全なインベントリを有していると報告している一方で、個人を特定できる情報（PII）またはクレジットカードの詳細などの機微な情報を返す API を特定できるのはこの 67% のうちの**わずか** *29%* です。

小売企業の中央 IT チームやセキュリティチームの連携や監視なしにビジネスユニットによって展開された API に起こり得ることを検討してみましょう。

- 顧客データを返すように設計されているが、適切な認証管理がなく、設定ミスに対するテストも適切に行われていない
- 新しいバージョンに置き換えられたが、無効化されていないため、インターネットへの露出が続いている
- 未管理の API を検知できない従来のツールに見過ごされる
- 詐欺師が実際の顧客のロイヤルティアカウントにアクセスし、現金に引き換えるなど悪用される

68% - 過去 12 か月間に API セキュリティインシデントを経験した小売／ E コマース企業の割合 [1]

わずか 29% - API の完全なインベントリを有する小売／ E コマース企業のうち、機微な情報を返す API を認識している企業の割合 [1]

$526,531 - 過去 12 か月間に小売／ E コマース企業が経験した API セキュリティインシデントの財務的影響 [1]

影響の上位 3 つ [1]

1. チームや部門に対する**ストレスやプレッシャーの増加**
2. 問題解決のための**コストが発生**
3. シニアリーダーや取締役会からの**部門への評判が低下**

44% - コマース組織に対する Web 攻撃のうち API を標的にした攻撃の割合 [2]

出典：
1. Akamai「API セキュリティの影響に関する調査」（2024）
2. Akamai のインターネットの現状（SOTI）、「影に潜む脅威：攻撃トレンドで API の脅威を解き明かす」（2024）

Akamai

このようなシナリオは単なる仮説ではありません。LexisNexis® Risk Solutions 社の「2023 True Cost of Fraud™ Study（真の詐欺のコストに関する調査）」によると、不正行為による損失の 50% は新規口座開設の不正利用に遡る可能性があり、詐欺師は大規模に口座を開設するために API を悪用しています。さらに、これらのシナリオには、実際の IT とセキュリティに挙げられた API インシデントの主な原因が反映されています。

小売／ E コマース企業のセキュリティチームが挙げる API インシデントの主な原因

1. 生成 AI ツール（LLM など）内の API – **24.7%**
2. API のインターネットへの意図しない露出 – **24.0%**
3. API の設定ミス – **22.0%**
4. Web アプリケーションファイアウォールによって捕捉されなかった – **21.3%**
5. API ゲートウェイによって捕捉されなかった – **20.7%**
6. API コーディングエラーによる脆弱性 – **20.0%**
7. よく知られたテクノロジーツール／サービス – **20.0%**
8. ネットワークファイアウォールによって捕捉されなかった – **18.7%**
9. 認可の脆弱性 – **17.3%**
10. インターネットからダウンロードしたソフトウェアソリューション – **16.7%**
11. API 認証制御の欠如 – **16.0%**
12. ミッドティア・ソフトウェア・ソリューション – **14.7%**
13. 未管理 API（ゾンビなど） – **13.3%**

Q. **貴社が経験した** *API* **セキュリティインシデントの原因は何だと思いますか？（***3* **つまで選択可）、** *n = 1,207*

API インシデントがコンプライアンス、ビジネスコスト、チームのストレスに与える影響

2024 年 5 月の「Gartner® API Market Guide for API Protection」によると、「現在のデータは、平均的な API 侵害によって漏えいするデータ量は平均的なセキュリティ侵害の 10 倍以上であることを示しています[3]。」広く採用されている PCI DSS v4.0 規制に API セキュリティに関する要件が追加されたのはもっともなことです。企業とその規制当局は、自組織の API だけでなく、パートナーやサプライヤーの API を介してどのようなタイプのデータが受送信されているかを把握する必要があります。これは、E コマースのサードパーティリスクを管理するためのあと 1 つの課題となります。

規制当局の信頼を失うことにより、監視が強化され、コンプライアンス要件対応に追われ、すでに疲弊しているチームにさらに大きな負担がかかる可能性があります。また、高額な罰金が科せられる可能性もあります。また、コストを考慮に入れると、小売企業や E コマース企業が API の脅威による経済的な影響を十分に認識していることは明らかです。今回初めて、調査対象の 3 か国において、過去 12 か月間に経験した API セキュリティインシデントによる推定の財務的影響を、回答者に尋ねました。

[3] GARTNER は、Gartner, Inc. またはその関連会社の米国およびその他の国における登録商標およびサービスマークであり、同社の許可に基づいて使用しています。All rights reserved.

	小売／ E コマース	全業界の平均
米国	$526,531	$591,404
英国	£258,815	£420,103
ドイツ	€ 348,467	€ 403,453

Q. API **セキュリティインシデントを経験したことがある場合、これらのインシデントの合計財務的影響の推定値はどのようなものでしたか？システムの修理、ダウンタイム、法的費用、罰金、その他の関連費用など、関連するすべての費用を含めてください、** *n = 1,207*

財務的な影響は大きいものの、調査参加者から明確に聞かれたのは、費用以上の負担があるということでした。API セキュリティインシデントの最大の影響を挙げるように求められたとき、挙げられたのは費用ではありませんでした。小売および E コマース業界の回答者が強調したのは、「チームにストレスとプレッシャーをかける」という人的負担でした。

小売企業および E コマース企業に対する API セキュリティインシデントの主な影響トップ 5

1. チームや部門へのストレスやプレッシャーの増加につながった – **28.7%**
2. 問題解決のためにコストが発生 – **28.0%**
3. シニアリーダーや取締役会からの部門への評判が低下 – **25.3%**
4. 事業部門間でのチームや部門への社内精査の増加につながった – **23.3%**
5. 規制当局からの罰金 – **25.3%**

Q. API ***セキュリティインシデントがビジネスにもたらしたコストや影響が何かあれば、それは何ですか？（3 つまで選択可）、****n = 1,207*

次のステップ：プロアクティブな API セキュリティでリスクとストレスを軽減

小売企業や E コマース企業に対する API 攻撃の範囲、規模、巧妙さが増しています。これには、従来の API セキュリティツールやその他の境界防御を回避するために迅速に適応する、生成 AI を利用したボット攻撃が含まれます。業界の多くのセキュリティチームは、これらの脅威を直接経験し、その財務的および人的な影響を感じています。しかし、組織が API の脅威の重要性を理解していても、それに対して何ができるのか、という疑問が残ります。

API とそれらが交換するデータのセキュリティを確保するために今すぐ対策を講じることで、企業は自社の収益を保護し、セキュリティチームの負担を軽減すると同時に、取締役会や顧客からの信頼を維持できます。これらのステップには、高度な API の脅威に関するチームの知識と、それらに対する防御に必要な機能を構築することが含まれます。

2024 年の API セキュリティの影響に関する調査をダウンロードいただき、レポートの全文で API の可視性と保護に関するベストプラクティスをご確認ください。

貴社の課題や Akamai が提供するサポートついてのご相談

カスタマイズされた Akamai API Security のデモをリクエスト

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。公開日：2024 年 11 月。