ブラウザー内保護に関する７つの誤解

インターネットで Web 対応のアプリケーションや資産が多様で複雑なサイバー攻撃にさらされることは、よく知られています。企業は、ミッションクリティカルなアプリケーションをサーバー側の攻撃から保護することに重点を置いていますが、ブラウザー内または Web ページ内でクライアント側の脅威によって生じる可能性のある損害を過小評価している企業は少なくありません。この盲点によりウェブサイトは、不正行為、機微な情報の窃盗、顧客からの信頼の喪失につながり得る、クライアント側の危険な脆弱性にさらされています。

ブラウザー内の保護に関するよくある誤解をいくつか解消して、実際に何が危機にさらされているのかを明確に把握することが重要です。

誤解 1

コンテンツ・セキュリティ・ポリシー（CSP）は非常に効果的なクライアント側防御

コンテンツ・セキュリティ・ポリシーは、どのアセット（スクリプトなど）をブラウザー内で実行できるかを Web サイトの運営者が詳細に制御できるセキュリティ標準です。コンテンツ・セキュリティ・ポリシーの応答ヘッダーは、実行コードの正当で安全なソースとみなされる、承認済みドメインのリストを維持するために使用されます。これは JavaScript の脅威に対する防御の重要な部分となる可能性がありますが、維持には膨大なリソースが必要です。また、クライアント側のほとんどの攻撃は、信頼性の高いソースを利用しているにもかかわらず発生しています。そのため、たとえ信頼の高いスクリプトであっても、サイトで実行されているすべてのスクリプトのふるまいを把握することが重要です。Akamai Page Integrity Manager は、ふるまいテクノロジーを活用して Web ページにおけるすべてのスクリプト実行動作を監視し、スクリプトのアクションや、他のスクリプトとの関係に関する情報を収集します。その後このデータを、ヒューリスティック、リスクスコアリング、人工知能など、多層的な検知アプローチと組み合わせて、疑わしいアクティビティを即座に特定します。

現在、

94%

の Web サイトが少なくとも 1 つのサードパーティースクリプトを利用しています

出典：サードパーティー、2021 年 11 月

誤解 2

WAF は Web スキミング攻撃から企業を守る

Web アプリケーションファイアウォール（WAF）は、一般的な攻撃から Web アプリケーションを保護するために、トラフィックの監視とフィルタリングに加え、Web アプリケーションに入る悪性トラフィックやアプリから出る不正なデータのブロックを行うセキュリティソリューションです。WAF はサーバーとエンドユーザー間の接続を保護することに重点を置いていますが、ブラウザーレベルで Web アプリケーションを保護するようには作られていません。Web スキミング攻撃は、悪性のコードの実行によってエンドユーザーのブラウザー内で発生するため、WAF では検知も緩和もできません。

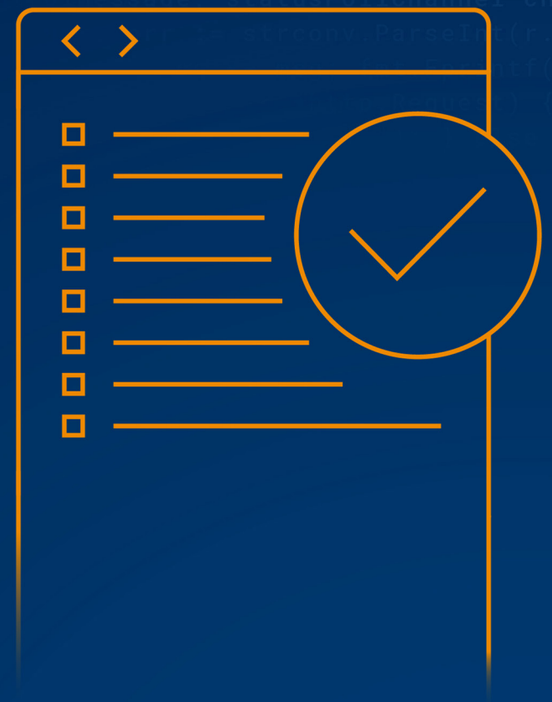
誤解 3

現在、Magecart 攻撃は、かつてほど頻繁には発生していない

Magecart 攻撃はかつてないほど活発化しており、検知が困難になっています。Akamai の脅威リサーチチームは先日、Google Tag Manager などの有名なサードパーティーベンダーになりすましたり、Base64 エンコーディングを使用して悪性のコードをカモフラージュしたりするなど、高度な技術を駆使して複数の E コマースサイトをターゲットにしたグローバルな Magecart キャンペーンを発見しました。これはいたちごっこであり、攻撃者はセキュリティ対策を回避して検知されないように Web スキミング攻撃を実行する方法に磨きをかけています。Akamai Page Integrity Manager はスクリプトのすべてのふるまいを監視し（スクリプトが他のスクリプトとどのようにやり取りして疑わしいアクティビティを暴くかを含む）、非常に高度な攻撃を迅速に防ぎます。詳細については、Akamai の最近のブログ記事をご覧ください。

誤解 4

PCI DSS v4.0 の新しいスクリプト要件への対応は急がなくてもよい



2022 年 3 月に最新バージョンの PCI DSS（v4.0）がリリースされました。決済カードデータに対する脅威の進化や、2018 年の PCI DSS v3.2.1 のリリース以降に発生した重要な市場の変化に対処することが目的です。新しい要件 6.4.3 および 11.6 の一部として、オンラインで決済カードを処理する企業は、ブラウザー内スクリプト攻撃を防止するために、サイトでどのスクリプトが実行されるか、そのスクリプトがいつ変更されるか、その各スクリプトの実行がいつ停止されるかを把握しなければならなくなりました。PCI DSS v4.0 の効力が生じるのは 2025 年以降ですが、機密性の高い決済カードデータが Web サイトの支払いページからスキミングされたり流出するリスクを防止するのを先延ばしにするわけにはいきません。Akamai の Page Integrity Manager を利用すれば、今すぐに PCI コンプライアンスを迅速化できます。

誤解 5

オンライン小売企業にとってオーディエンスハイジャックは大きな課題ではない

オーディエンスハイジャックとは、クライアント側にインストールされているブラウザー拡張機能やプラグインの結果として発生する、望ましくないまたは悪性のブラウザーアクティビティを表す用語です。こうした望ましくないアクティビティとしては、アフィリエイト詐欺、競合サイトや悪性サイトへの不正なリダイレクト、意図しない割引、訪問者が購入を完了できないようにする邪魔な広告挿入などがあります。企業は自社 Web サイトの合計アクセス者数の 15%～24% が、オーディエンスハイジャック戦略によって妨げられていると予測しています。

これによってどのようなことが起こるのでしょうか？コンバージョン率の低下、ブランドロイヤルティの低下、何百万ドルもの潜在収益の損失です。Akamai Audience Hijacking Protector を使用すると、ブラウザーのよくある拡張機能がサイトセッションにどのように影響を与えているか、また、拡張機能の操作者が悪性のアクティビティをどのように実行しているかを把握できます。これは、拡張機能レベルで詳細なポリシー設定を使用してアクティビティをブロックまたは許可することにより、どの拡張機能とサイトのインタラクションを許可するかを決めるうえで役立ちます。

企業は自社 Web サイトの合計アクセス者数の

15%～24%

が、オーディエンスハイジャック戦略によって妨げられていると予測しています

出典：オンライン小売企業内でのオーディエンスハイジャックの認知度、Retail Dive、2023 年 2 月

誤解 6

デジタル体験プラットフォームによって、ブラウザー内のアクティビティとブラウザー拡張機能の影響を可視化できる

デジタル体験プラットフォームは、コンテンツ主導の体験を最適化して提供するために連携する一連のテクノロジーです。このようなプラットフォームから現在得られるアナリティクスは、サイトセッションのエンドユーザー側ではなく企業側で発生していることについてのみ知見をもたらします。つまり、サイトにアクセスした人がサイトとどのようにやり取りしているか、およびそのふるまいを追跡することはできても、ブラウザーがエンドユーザーとどのようにやり取りしているかを可視化することはできません。ブラウザーの拡張機能や不要なブラウザーアクティビティがサイトセッションにどのように影響するかを把握することで、カスタマージャーニー全体を総合的に把握し、カート離脱の理由をより明確にすることできます。

誤解 7

クーポンや価格比較の拡張機能がビジネスに害を及ぼすことはない

これは難しい問題です。お買い得の商品を好むのは誰でも同じであり、オンライン小売店のコンバージョン率を高めるためには、Honey、楽天、Amazon Assistant などの拡張機能が役立ちます。しかし、こうした拡張機能にはマイナス面もあります。たとえば、クーポン拡張機能は、対象外のユーザーの支払いページにも限定割引コードを自動的に挿入し、大規模な割引を引き起こします。Amazon Assistant は、競合他社を介して自社の商品やサービスをより低価格で提供する広告を自社サイトに自動的に挿入します。このような拡張機能によって大幅な潜在収益損失が発生し、上顧客の喪失にもつながります。Akamai Audience Hijacking Protector は、世界で最も人気のある多数のブラウザー拡張機能をサポートしています。また、Akamai の高度なダッシュボードは、拡張機能ごとに知見を出力します。そのため、どの拡張機能が実際にビジネスに役立っているか、利用する価値がない拡張機能はどれかを分析できます。

Akamai のお客様のグローバル・サイト・トラフィック全体で、クーポンや価格比較の拡張機能によって影響を受けたサイトセッションの数が、ブラックフライデーとサイバーマンデーの間で

25%

増加しました

出典：Akamai の脅威リサーチ、2022 年

Akamai の役割

クライアント側の攻撃による影響を受けるリスクが急速に高まっていることは明らかです。リスクを軽減するためには、ブラウザー内のふるまいや不要なアクティビティを可視化することが極めて重要です。Akamai の Page Integrity Manager は、脆弱なリソースを特定し、疑わしいふるまいを検知し、悪性のアクティビティをブロックすることで、ウェブスキミング、フォームジャッキング、Magecart 攻撃など JavaScript の脅威から Web サイトを保護します。また、ブラウザー内の不要なふるまいを阻止するために、Audience Hijacking Protector は詳細な分析と緩和のオプションによって、デジタル商取引サイトで発生しているブラウザーアクティビティをリアルタイムで可視化します

Akamai のアプリケーション防御、API 防御、ブラウザー内保護ソリューションが、クライアント側のセキュリティ対策の改善にどのように役立つかをご説明します。