Les 7 mythes sur la protection intégrée au navigateur

Ce n'est un secret pour personne qu'Internet expose les applications et les ressources Web à une multitude de cyberattaques complexes et diverses. Les entreprises mettent l'accent sur la protection de leurs applications stratégiques contre les attaques côté serveur, mais beaucoup sous-estiment les dommages qui peuvent être causés par les menaces côté client au sein du navigateur ou de la page Web elle-même. Cette zone d'ombre expose les sites Web à de dangereuses failles côté client, qui peuvent mener à la fraude et à l'exfiltration de données sensibles, et ainsi entamer la confiance des clients.

Nous allons examiner quelques-unes des idées reçues les plus courantes sur la protection intégrée au navigateur pour nous faire une meilleure idée des enjeux réels.

Mythe 1

Une politique de sécurité du contenu (CSP) est la défense côté client la plus efficace

Une politique de sécurité du contenu est une norme de sécurité qui permet aux opérateurs de sites Web d'assurer un contrôle granulaire des ressources pouvant être exécutées dans le navigateur, notamment les scripts. Les en-têtes de réponse des politiques de sécurité du contenu sont utilisés pour gérer une liste de domaines approuvés considérés comme des sources légitimes et sûres de code exécutable. Ils peuvent constituer un élément essentiel de votre défense contre les menaces JavaScript, mais ils impliquent l'utilisation d'une multitude de ressources – et la plupart des attaques côté client se produisent en exploitant des sources fiables. C'est pourquoi il est important de comprendre le comportement de tous les scripts exécutés sur votre site, même celui des scripts de confiance. La solution Page Integrity Manager d'Akamai tire parti de la technologie comportementale pour surveiller tous les comportements d'exécution de scripts sur une page Web, en recueillant des informations sur les actions des scripts et leurs relations avec d'autres scripts. Elle associe ensuite ces données à une approche de détection multicouches (notamment l'heuristique, l'évaluation des risques, l'intelligence artificielle et d'autres facteurs) pour identifier immédiatement les activités suspectes.

À l'heure actuelle,

94 %

des sites Web utilisent au moins un script tiers

Source : Tiers, novembre 2021

Mythe 2

Un WAF protège mon entreprise contre les attaques de web skimming

Un pare-feu d'applications Web (WAF) est une solution de sécurité qui protège les applications Web contre les attaques courantes en surveillant et en filtrant le trafic, en bloquant le trafic malveillant entrant dans une application Web ou les données non autorisées quittant l'application. Les WAF se concentrent sur la protection de la connexion entre vos serveurs et les utilisateurs finaux, mais ils ne sont pas conçus pour protéger votre application Web au niveau du navigateur. Les attaques de web skimming se produisant au sein du navigateur de l'utilisateur final au moyen de l'exécution de code malveillant, les WAF sont incapables de les détecter ou de les atténuer.

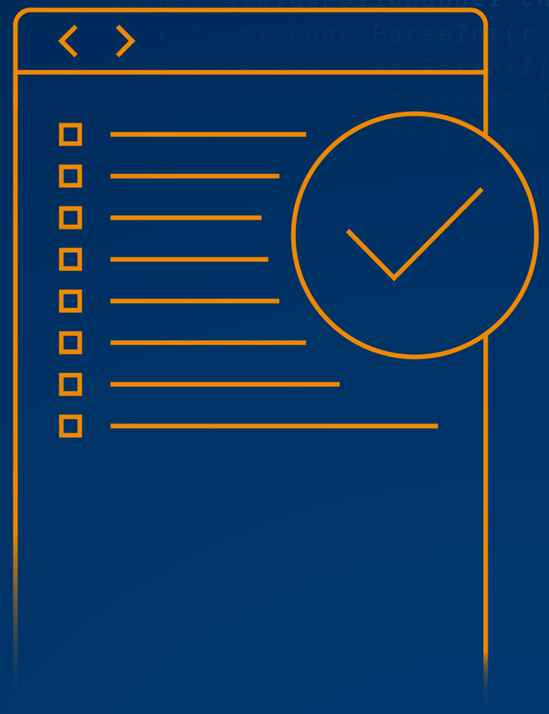
Mythe 3

Les attaques Magecart ne sont plus aussi fréquentes qu'autrefois

Les attaques Magecart sont plus actives que jamais – elles sont simplement de plus en plus difficiles à détecter. L'équipe de recherche sur les menaces d'Akamai a récemment découvert une campagne Magecart mondiale qui ciblait plusieurs sites de commerce électronique à l'aide de techniques sophistiquées, telles que l'usurpation d'identité d'un fournisseur tiers connu comme Google Tag Manager ou l'utilisation de l'encodage Base64 pour masquer les codes malveillants. C'est un jeu du chat et de la souris, où les cybercriminels tentent de contourner les mesures de sécurité et d'exécuter leurs attaques de web skimming de manière plus intelligente pour ne pas être détectés. Pour identifier toute activité suspecte, Page Integrity Manager d'Akamai surveille tous les comportements des scripts, y compris la manière dont ils interagissent avec d'autres scripts, pour offrir une protection rapide contre les attaques les plus avancées. Pour en savoir plus, consultez notre récent article de blog.

Mythe 4

J'ai du temps pour me conformer aux nouvelles exigences de script de la norme PCI DSS v4.0



En mars 2022, la dernière version de la norme PCI DSS (v4.0) a été publiée pour faire face aux menaces en constante évolution concernant les données des cartes de paiement et aux importants changements du marché qui se sont produits depuis la version précédente de la norme PCI DSS v3.2.1 en 2018. Dans le cadre des nouvelles exigences 6.4.3 et 11.6, toute entreprise traitant des cartes de paiement en ligne doit désormais savoir quels scripts s'exécutent sur son site, quand ces scripts changent et quand chacun de ces scripts cesse de s'exécuter, pour se défendre contre les attaques de script dans le navigateur. Même si la norme PCI DSS v4.0 ne prendra effet qu'en 2025, vous ne pouvez pas vous permettre de remettre à plus tard la protection des données de paiement sensibles contre le vol et l'extraction depuis les pages de paiement de votre site Web. La solution Page Integrity Manager d'Akamai peut vous aider à accélérer la conformité PCI dès aujourd'hui.

Mythe 5

Le détournement d'audience n'est pas un défi majeur pour les commerçants en ligne

Le détournement d'audience est le terme utilisé pour décrire les activités de navigateur indésirables et parfois malveillantes qui se produisent suite à l'installation d'extensions de navigateur ou de plug-ins côté client. Ces activités indésirables peuvent inclure la fraude d'affiliation, les redirections non autorisées vers des sites concurrents ou malveillants, les remises non intentionnelles et les injections publicitaires indésirables qui risquent d'empêcher un visiteur de réaliser un achat. Les entreprises estiment que 15 à 24 % du total des visites sur leur site Web sont perturbées par des tactiques de détournement d'audience.

Par quoi cela peut-il se traduire ? Des taux de conversion plus faibles, une baisse de la fidélité envers la marque et des pertes de revenus potentiels qui se chiffrent en millions. Audience Hijacking Protector d'Akamai permet aux utilisateurs de mieux comprendre l'impact des extensions de navigateur courantes sur les sessions, ainsi que le mode opératoire des opérateurs d'extension. Cette solution vous permet de décider quelles extensions sont autorisées à interagir avec votre site en mettant en place des règles granulaires au niveau de l'extension individuelle pour bloquer ou autoriser l'activité.

Les entreprises estiment que

15 à 24 %

du total des visites sur leur site Web sont perturbées par des tactiques de détournement d'audience

Source : Awareness of Audience Hijacking Among Online Retailers, Retail Dive, février 2023

Mythe 6

Les plateformes d'expérience digitale permettent d'avoir une visibilité sur les activités du navigateur et sur l'impact des extensions de navigateur

Une plateforme d'expérience digitale est un ensemble de technologies qui travaillent ensemble pour offrir des expériences axées sur le contenu et les optimiser. Les analyses actuelles de ces plateformes fournissent uniquement des informations sur ce qui se passe du côté entreprise d'une session, et non du côté de l'utilisateur final. Vous pouvez donc suivre l'interaction d'un visiteur avec votre site et ses comportements, mais vous n'avez aucune visibilité sur la façon dont le navigateur interagit avec l'utilisateur final. En comprenant comment les extensions de navigateur et les activités de navigateur indésirables peuvent affecter les sessions sur votre site, vous bénéficiez d'un aperçu complet de l'ensemble du parcours client, qui vous permet de mieux définir les raisons de l'abandon de panier.

Mythe 7

Les extensions de coupons et de comparaison de prix ne nuisent pas à mon entreprise

Nous sommes bien conscients qu'il s'agit d'une question délicate. Tout le monde aime faire de bonnes affaires, et des extensions comme Honey, Rakuten et Amazon Assistant peuvent aider les commerçants en ligne à optimiser leurs taux de conversion. Mais ces extensions peuvent avoir une face sombre. Prenons l'exemple d'une extension de coupon qui insère automatiquement un code d'offre exclusive dans la page de paiement d'utilisateurs n'appartenant pas à votre audience cible, ce qui entraîne des remises massives. Ou d'Amazon Assistant qui injecte automatiquement sur votre site une publicité offrant un produit ou un service absolument identique au vôtre, fourni à un prix inférieur par un concurrent. Ces extensions peuvent entraîner des pertes de revenus importantes et détourner vos clients les plus fidèles. Audience Hijacking Protector d'Akamai prend en charge des dizaines d'extensions de navigateur parmi les plus utilisées au monde, et notre tableau de bord avancé fournit des informations au niveau de l'extension individuelle, ce qui permet aux utilisateurs d'analyser les extensions qui sont réellement bénéfiques à l'entreprise et celles qui ne valent pas la peine d'être autorisées.

Sur l'ensemble du trafic des clients d'Akamai, le nombre de sessions affectées par des extensions de coupons et de comparaison de prix a augmenté de

25 %

entre le Black Friday et le Cyber Monday

Source : Recherches sur les menaces d'Akamai, 2022

Comment Akamai peut vous aider

Le risque d'être affecté par une attaque côté client s'accélérant, il est essentiel d'accroître la visibilité sur les comportements et les activités indésirables au sein du navigateur pour réduire cette menace. Page Integrity Manager protège les sites Web contre les menaces Javascript, telles que le vol de données de cartes bancaires (web skimming), le détournement de formulaires (form jacking) et les attaques Magecart, en identifiant les ressources les plus vulnérables, en détectant les comportements suspects et en bloquant les activités malveillantes. Et pour empêcher les comportements indésirables au sein du navigateur, Audience Hijacking Protector fournit une visibilité en temps réel sur les activités de navigateur qui se déroulent sur votre site de commerce digital, avec des options d'analyse granulaire et d'atténuation.

Découvrez comment les défenses d'applications et d'API ainsi que les solutions de protection intégrée au navigateur d'Akamai peuvent vous aider à améliorer les stratégies de sécurité côté client.