
Akamai
Os sete mitos
da proteção no
navegador

Não é segredo que a Internet expõe aplicações e ativos voltados para a Web a uma variedade complexa de ataques cibernéticos. Embora as organizações coloquem um foco significativo na proteção de suas aplicações essenciais contra ataques no lado do servidor, muitas subestimam os danos que podem ser causados por ameaças no lado do cliente dentro do navegador ou dentro da própria página da Web. Esse ponto cego deixa os websites expostos a vulnerabilidades perigosas no lado do cliente que podem levar a fraudes, exfiltração de dados confidenciais e danos à confiança do cliente.

Vamos analisar separadamente algumas das concepções erradas comuns da proteção no navegador para ter uma visão mais clara do que realmente está em jogo.

Mito 1

Uma CSP (Política de Segurança de Conteúdo) é a defesa mais eficaz do lado do cliente

Uma Política de Segurança de Conteúdo é um padrão de segurança que permite que os operadores de websites controlem de forma granular quais ativos podem ser executados dentro do navegador, incluindo scripts. Os cabeçalhos de resposta da Política de Segurança de Conteúdo são usados para manter uma lista de domínios aprovados considerados fontes legítimas e seguras de código executável. Eles podem ser uma parte crítica de sua defesa contra ameaças JavaScript, mas exigem muitos recursos para sua manutenção, e a maioria dos ataques do lado do cliente ocorre ao aproveitar fontes confiáveis. Por isso, é importante compreender o comportamento de todos os scripts em execução no seu website, mesmo os confiáveis. O Akamai Page Integrity Manager aproveita a tecnologia comportamental para monitorar todo o comportamento de execução de scripts em uma página da Web, coletando inteligência sobre as ações dos scripts e seus relacionamentos com outros scripts. Em seguida, ele combina esses dados com uma abordagem de detecção em multicamadas que inclui heurística, pontuação de risco, inteligência artificial e muito mais para identificar imediatamente atividades suspeitas.

94%

dos websites hoje aproveitam pelo menos um script de terceiros

Fonte: Terceiros, novembro de 2021

Mito 2

Um WAF protege minha organização contra ataques de skimming da Web

Um WAF (firewall de aplicações Web) é uma solução de segurança que protege as aplicações Web contra os ataques comuns monitorando e filtrando o tráfego ou bloqueando a entrada de tráfego mal-intencionado em uma aplicação da Web ou a saída de dados não autorizados do app. Os WAFs estão focados em proteger a conexão entre seus servidores e usuários finais, mas não foram projetados para proteger sua aplicação da Web no nível do navegador. Como os ataques de skimming da Web ocorrem no navegador do usuário final por meio da execução de código mal-intencionado, os WAFs não conseguem detectar nem mitigar.

Mito 3

Os ataques de Magecart não acontecem com tanta frequência hoje quanto no passado

Os ataques de Magecart estão mais vivos do que nunca e cada vez mais difíceis de detectar. Recentemente, nossa equipe de Pesquisa de ameaças da Akamai descobriu uma campanha global da Magecart que visava vários websites de comércio eletrônico usando técnicas sofisticadas, como fazer-se passar por um conhecido fornecedor terceirizado, como o Google Tag Manager ou usar a codificação Base64 para camuflar um código mal-intencionado. É um jogo de gato e rato, em que os agentes de ameaça tentam contornar as medidas de segurança e ficar mais inteligentes sobre como executam ataques de navegação na Web para permanecerem indetectáveis. O Akamai Page Integrity Manager monitora todos os comportamentos dos scripts, incluindo como eles interagem com outros scripts para expor qualquer atividade suspeita, e defende rapidamente até mesmo contra os ataques mais avançados. Saiba mais em nossa publicação recente no blog.

Mito 4

Posso esperar para estar em conformidade com os novos requisitos de script para o PCI DSS v4.0

Em março de 2022, a versão mais recente do PCI DSS (v4.0) foi lançada para lidar com ameaças em evolução aos dados de cartões de pagamento e alterações críticas do mercado que ocorreram desde a versão anterior do PCI DSS v3.2.1 em 2018. Como parte dos novos requisitos 6.4.3 e 11.6, qualquer organização que processa cartões de pagamento online deve agora saber quais scripts são executados em seu website, quando esses scripts são alterados e quando cada um deles para de funcionar, para se defender contra ataques de script no navegador. Embora o PCI DSS v4.0 não entre em vigor até 2025, você não pode se dar ao luxo de atrasar a proteção de dados confidenciais de cartões de pagamento contra roubo e exfiltração das páginas de pagamento do seu website. O Akamai Page Integrity Manager pode ajudar a acelerar a conformidade com PCI hoje mesmo.

Mito 5

O sequestro de público não é um grande desafio para os varejistas online

Sequestro de público é o termo usado para descrever atividades indesejadas e, às vezes, mal-intencionadas do navegador que ocorrem como resultado de extensões ou plug-ins do navegador instalados no lado do cliente. Essas atividades indesejadas podem incluir fraude de afiliados, redirecionamentos não autorizados para websites concorrentes ou maliciosos, descontos não intencionais e injeções de anúncios que podem impedir que um visitante conclua uma compra. As organizações estimam que 15% a 24% do total de visitas a seus websites são interrompidas por táticas de sequestro de público.

O que isso pode representar? Taxas de conversão mais baixas, uma diminuição na fidelidade à marca e milhões perdidos em receita potencial. O Akamai Audience Hijacking Protector permite que os usuários tenham visibilidade de como as extensões comuns do navegador estão afetando as sessões do website, da mesma forma como os operadores de extensão podem estar conduzindo atividades mal-intencionadas. Ele permite que você decida quais extensões podem interagir com seu website, usando a configuração de política granular no nível de extensão individual para bloquear ou permitir a atividade.

As organizações estimam que

15% a 24%

do total de visitas a seus websites são interrompidas por táticas de sequestro de público

Fonte: Awareness of Audience Hijacking Among Online Retailers, Retail Dive, fevereiro de 2023

Mito 6

As plataformas de experiência digital podem fornecer visibilidade das atividades no navegador e dos impactos das extensões do navegador

Uma plataforma de experiência digital é um conjunto de tecnologias que trabalham juntas para otimizar e oferecer experiências orientadas por conteúdo. A análise atual que é fornecida a partir dessas plataformas fornece apenas percepções sobre o que está ocorrendo no lado da organização de uma sessão do website, e não no lado do usuário final. Isso significa que, embora você possa rastrear como um visitante do website está interagindo com seu website e seus comportamentos, você não tem visibilidade de como o navegador pode estar interagindo com o usuário final. Ao entender como as extensões do navegador e as atividades indesejadas do navegador podem estar afetando as sessões do website, você tem uma visão abrangente de toda a jornada do cliente e pode definir melhor os motivos para o abandono do carrinho de compras.

Mito 7

Extensões de comparação de cupons e preços não são prejudiciais para minha empresa

Isso é complicado, nós entendemos. Todos adoram um bom negócio, e extensões como Honey, Rakuten e Amazon Assistant podem ajudar os varejistas online a impulsionar as taxas de conversão. No entanto, essas extensões podem ter um lado mais sombrio. Considere, por exemplo, uma extensão de cupom que insere automaticamente um código de oferta exclusivo na página de finalização de compra de usuários fora do público-alvo, causando descontos em massa. Ou o Amazon Assistant injetando automaticamente um anúncio em seu website oferecendo o exato produto ou serviço que você oferece a um preço mais baixo por meio de um concorrente. Essas extensões podem levar a uma perda significativa de receita potencial e levar até seu cliente mais fiel a se desviar. O Akamai Audience Hijacking Protector suporta dezenas de extensões dos navegadores mais populares do mundo, e nosso painel avançado fornece insights no nível de extensão individual, permitindo que os usuários analisem quais extensões são realmente benéficas para a empresa e quais não valem a pena permitir.

No tráfego global de clientes da Akamai no website, o número de sessões impactadas por extensões de comparação de cupons e preços aumentou

25%

entre a Black Friday e a Cyber Monday

Fonte: Pesquisa da Akamai sobre ameaças, 2022

Como a Akamai pode ajudar

Fica claro que o risco de ser afetado por um ataque no lado do cliente está acelerando, e obter visibilidade dos comportamentos no navegador e das atividades indesejadas é fundamental para reduzir o risco. O Page Integrity Manager da Akamai protege websites contra ameaças de Javascript, como web skimming, formjacking e ataques de Magecart, identificando recursos vulneráveis, detectando comportamentos suspeitos e bloqueando atividades mal-intencionadas. E para interromper comportamentos indesejados no navegador, o Audience Hijacking Protector fornece visibilidade em tempo real das atividades do navegador que ocorrem em seu website de comércio digital com análise granular e opções de mitigação

Saiba como as aplicações da Akamai e as defesas de APIs e as soluções de proteção no navegador da Akamai podem ajudar você a melhorar as posturas de segurança no lado do cliente.