Los 7 mitos sobre la protección integrada en el navegador

No es ningún secreto que Internet expone las aplicaciones y los activos web a una amplia y compleja variedad de ciberataques. Mientras se centran en proteger sus aplicaciones esenciales contra los ataques en el lado del servidor, muchas organizaciones subestiman el daño que pueden causar las amenazas en el lado del cliente dentro del navegador o dentro de la propia página web. Este punto ciego deja los sitios web expuestos a peligrosas vulnerabilidades del lado del cliente que pueden dar lugar a fraudes, a la exfiltración de datos confidenciales y a la pérdida de la confianza de los clientes.

Desmontemos algunas de las ideas erróneas comunes sobre la protección en el navegador para tener una idea más clara de lo que realmente está en juego.

Mito n.º 1

Una política de seguridad del contenido (CSP) es la defensa más eficaz del lado del cliente

Una política de seguridad de contenido es un estándar de seguridad que permite a los operadores del sitio web controlar con detalle qué activos se pueden ejecutar en el navegador, incluidos los scripts. Los encabezados de respuesta de las políticas de seguridad de contenido se utilizan para mantener una lista de dominios aprobados que se consideran fuentes legítimas y seguras de código ejecutable. Pueden ser una parte fundamental de su defensa contra las amenazas de JavaScript, pero requieren el mantenimiento de una gran cantidad de recursos y la mayoría de los ataques del lado del cliente se produce mientras se utilizan fuentes de confianza. Por eso es importante comprender el comportamiento de todos los scripts que se ejecutan en su sitio, incluso los de confianza. Page Integrity Manager de Akamai usa tecnología conductual para supervisar todo el comportamiento de ejecución de scripts en una página web, recopilando información sobre las acciones de los scripts y sus relaciones con otros scripts. A continuación, combina esos datos con un enfoque de detección multicapa que incluye heurística, puntuación de riesgos, inteligencia artificial y mucho más, con el fin de identificar inmediatamente actividades sospechosas.

94 %

de los sitios web utiliza actualmente al menos un script de terceros

Fuente: Third Parties, noviembre de 2021

Mito n.º 2

Un WAF protege a mi organización contra ataques de robo de información web

Un firewall de aplicaciones web (WAF) es una solución de seguridad que protege las aplicaciones web de ataques comunes mediante la supervisión y el filtrado del tráfico, el bloqueo del tráfico malicioso que entra en una aplicación web o la salida de datos no autorizados de la aplicación. Los WAF se centran en proteger la conexión entre los servidores y los usuarios finales, pero no están diseñados para proteger la aplicación web a nivel de navegador. Debido a que los ataques de robo de información web se producen en el navegador del usuario final mediante la ejecución de código malicioso, los WAF no pueden detectarlos ni mitigarlos.

Mito n.º 3

Los ataques de Magecart no son actualmente tan frecuentes como en el pasado

Los ataques de Magecart están más activos que nunca y son cada vez más difíciles de detectar. Recientemente, el equipo de investigación de amenazas de Akamai descubrió una campaña global de Magecart dirigida a varios sitios de comercio electrónico mediante técnicas sofisticadas, como la suplantación de identidad de un proveedor externo conocido, como Google Tag Manager, o el uso de codificación Base64 para ocultar código malicioso. Se trata del juego del gato y el ratón, en el que los atacantes intentan eludir las medidas de seguridad y perfeccionar su forma de ejecutar ataques de robo de información web mientras siguen pasando inadvertidos. Para exponer cualquier actividad sospechosa, Page Integrity Manager de Akamai supervisa todos los comportamientos de los scripts, incluida la forma en que interactúan con otros scripts, y defiende rápidamente incluso contra los ataques más avanzados. Obtenga más información en nuestra reciente publicación en el blog.

Mito n.º 4

Aún hay tiempo para cumplir con los nuevos requisitos sobre scripts del estándar PCI DSS v4.0

En marzo de 2022, se publicó la última versión del estándar PCI DSS (v4.0) con el objetivo de afrontar las amenazas en constante evolución a los datos de las tarjetas de pago y los cambios críticos que se habían producido en el mercado desde la versión anterior del estándar PCI DSS v3.2.1 en 2018. Como parte de los nuevos requisitos 6.4.3 y 11.6, cualquier organización que procese tarjetas de pago online debe saber qué scripts se ejecutan en su sitio, cuándo cambian y cuándo dejan de ejecutarse cada uno de ellos, con el fin de defenderse de los ataques de scripts en el navegador. Aunque PCI DSS v4.0 no será aplicable hasta 2025, no puede demorar la protección de los datos confidenciales de las tarjetas de pago para evitar su robo y exfiltración en las páginas de pago de su sitio web. Page Integrity Manager de Akamai puede ayudarle a acelerar el cumplimiento en el sector de las tarjetas de pago hoy mismo.

Mito n.º 5

El secuestro de audiencias no es un problema importante para los retailers online

El secuestro de audiencias es el término utilizado para describir actividades del navegador no deseadas, en ocasiones maliciosas, que se producen como resultado de la instalación de extensiones de navegador o de complementos del lado del cliente. Estas actividades no deseadas pueden incluir fraude de afiliados, redirecciones no autorizadas a sitios de la competencia o maliciosos, descuentos no deseados e inyecciones de anuncios que distraen al visitante y pueden impedir que complete una compra. Las organizaciones estiman que entre el 15 % y el 24 % del total de visitas a sus sitios web se distraen con tácticas de secuestro de audiencias.

¿Cuáles pueden ser las consecuencias? Menores tasas de conversión, una disminución de la fidelidad a la marca y millones de pérdidas en ingresos potenciales. Audience Hijacking Protector de Akamai permite a los usuarios comprender mejor el impacto de las extensiones comunes del navegador en las sesiones del sitio y las posibles actividades maliciosas por parte de los operadores de extensiones. Le permite decidir qué extensiones pueden interactuar con su sitio mediante una configuración de directivas detallada en el nivel de extensión individual para bloquear o permitir la actividad.

Las organizaciones estiman que entre el

15 % y el 24 %

del total de visitas a sus sitios web se distraen con tácticas de secuestro de audiencias

Fuente: Awareness of Audience Hijacking Among Online Retailers, Retail Dive, febrero de 2023

Mito n.º 6

Las plataformas de experiencia digital pueden proporcionar visibilidad de las actividades en el navegador y del impacto de las extensiones del navegador

Una plataforma de experiencia digital es una combinación de tecnologías que funcionan conjuntamente para ofrecer experiencias basadas en contenido y optimizarlas. Los análisis actuales que se proporcionan desde estas plataformas solo incluyen información sobre lo que está ocurriendo en una sesión del sitio del lado de la organización, no del lado del usuario final. Esto significa que, aunque puede realizar un seguimiento de cómo interactúa un visitante con su sitio y cuál es su comportamiento, no tiene visibilidad de la interactuación del navegador con el usuario final. Al comprender cómo las extensiones y las actividades no deseadas del navegador pueden afectar a las sesiones del sitio, obtendrá una visión completa de todo el recorrido del cliente y podrá definir mejor los motivos por los que no finaliza la compra.

Mito n.º 7

Las extensiones de cupones y comparación de precios no son perjudiciales para mi negocio

Este es complejo, lo sabemos. A nadie le gusta dejar pasar una buena oferta y extensiones como Honey, Rakuten y Amazon Assistant pueden ayudar a los retailers online a aumentar las tasas de conversión. Sin embargo, estas extensiones pueden tener un lado oscuro. Tomemos, por ejemplo, una extensión de cupón que inserte automáticamente un código de oferta exclusivo en la página de pago de los usuarios no pertenecientes a su audiencia objetivo, provocando descuentos masivos. O imagine que Amazon Assistant inyecte automáticamente un anuncio en su sitio web ofreciendo exactamente su mismo producto o servicio a un precio más bajo a través de un competidor. Estas extensiones pueden provocar una importante pérdida de ingresos e incluso de los clientes más fieles. Audience Hijacking Protector de Akamai admite muchas de las extensiones de navegador más populares del mundo, y nuestro panel avanzado proporciona información de cada extensión individual, lo que permite a los usuarios analizar qué extensiones son realmente beneficiosas para la empresa y cuáles no merecen la pena.

En el tráfico global de los sitios de clientes de Akamai, el número de sesiones afectadas por las extensiones de cupones y comparación de precios aumentó un

25 %

entre el Black Friday y el Cyber Monday

Fuente: Centro de investigación de amenazas de Akamai, 2022

Cómo puede ayudar Akamai

Está claro que el riesgo de verse afectado por un ataque del lado del cliente se está acelerando, y obtener visibilidad de los comportamientos y la actividad no deseada en el navegador es fundamental para reducirlo. Page Integrity Manager de Akamai protege los sitios web de amenazas JavaScript, como el robo de información web, el formjacking y los ataques de Magecart, mediante la identificación de recursos vulnerables, la detección de comportamientos sospechosos y el bloqueo de actividades maliciosas. Para detener los comportamientos no deseados en el navegador, Audience Hijacking Protector proporciona visibilidad en tiempo real de las actividades del navegador que ocurren en su sitio de comercio digital, con opciones de análisis y mitigación detalladas.

Descubra cómo las defensas de API y aplicaciones de Akamai, así como sus soluciones de protección integradas en el navegador pueden ayudarle a mejorar las estrategias de seguridad del lado del cliente.