ESTUDIO SOBRE EL IMPACTO DE LA SEGURIDAD DE API DE 2024

Sector gubernamental

Los incidentes relacionados con las API aumentan. Descubra cómo está afrontando el sector gubernamental este importante problema de seguridad y qué puede hacer su organización para mantenerse a salvo.

Los gobiernos de todo el mundo sufren la creciente presión de proteger los servicios digitales en un contexto de gran importancia de las API. En 2024, el 86,1 % de las organizaciones del sector público registró un incidente de seguridad de API, lo que supone un aumento significativo respecto al 76,8 % del año anterior. Este incremento sitúa al sector público por encima de la media del 84 % de todos los sectores: de ahí la magnitud del reto, que abarca desde el cumplimiento de requisitos relativos al Reglamento General de Protección de Datos (RGPD) hasta la aplicación de la residencia de datos en los sistemas multinube y la lucha contra las amenazas de seguridad nacionales. Todos los organismos necesitan una mayor visibilidad, un control más sólido y una resiliencia integrada.

El coste real de los incidentes de seguridad de las API en organismos públicos

Los organismos gubernamentales están adoptando cada vez más las API para habilitar servicios digitales, facilitar el uso compartido de datos entre instituciones y modernizar la infraestructura. Sin embargo, esta tendencia ha introducido una serie de nuevas vulnerabilidades que los atacantes están dispuestos a explotar. Los mecanismos de autenticación deficientes, las configuraciones erróneas de las API y la falta de conocimiento de los indicadores de riesgo críticos han hecho que el sector público sea especialmente susceptible a las infracciones de seguridad de las API. Las consecuencias de estos incidentes van mucho más allá del robo de datos, ya que ponen en riesgo la continuidad operativa, el cumplimiento normativo y la confianza pública.

¿Cómo disponemos de esta información? Akamai ha encuestado a más de 1200 profesionales de TI y seguridad, desde directores de seguridad de la información hasta personal de seguridad de las aplicaciones, para conocer sus experiencias con las amenazas relacionadas con las API.

Estos fueron algunos de los principales comentarios de los encuestados con respecto a incidentes de seguridad de API en el sector gubernamental:

- "Aumento del estrés o la presión para el equipo o el departamento" (28,5 %)
- "Daños a la reputación de nuestro departamento ante los altos puestos y la junta directiva" (27,2 %)
- "Sanciones por parte de los reguladores" (25,2 %)

Estas repercusiones interrelacionadas se entienden fácilmente, dado que sus homólogos han estimado el coste de afrontar los incidentes de las API en 717 500 dólares, un 21,3 % más que el promedio de los ocho sectores encuestados.

Siga leyendo para obtener información específica de este sector en el Estudio sobre el impacto de la seguridad de API de 2024.

A medida que los ataques aumentan, la visibilidad se convierte en una preocupación cada vez mayor

Cuando se les pidió que citaran las principales causas de sus incidentes de seguridad de API, los encuestados identificaron dos vulnerabilidades clave:

- Falta de controles de autenticación de API (25,2 %)
- Protección de las API con herramientas tradicionales (25,2 %)

A pesar de las crecientes pruebas de las consecuencias de las amenazas de API, desde los elevados costes de corrección hasta la erosión de la confianza, nuestros resultados sugieren que muchos equipos gubernamentales aún no priorizan su seguridad. De hecho, esta cuestión ocupa el sexto lugar entre las prioridades de ciberseguridad para el próximo año, con un 17,9 %.

El 86,1 % de las organizaciones gubernamentales afirmó haber experimentado un incidente de seguridad de API en 2024, lo que supone un aumento significativo con respecto al 76,8 % de 2023

717 500 USD es el coste financiero medio de una infracción de seguridad de API para las organizaciones gubernamentales de Estados Unidos, lo que supera la media de 591 404 USD de todos los demás sectores

El 66,9 % de las entidades gubernamentales mantienen un inventario de API, aunque solo el 18,5 % tiene total visibilidad de las API que gestionan datos confidenciales, lo que pone en riesgo la información crítica

3 consecuencias principales

1. **Aumento del estrés o la presión para los equipos de seguridad**
2. **Daño a la reputación del equipo, incluidos los responsables y la junta directiva**
3. **Multas normativas por incumplimiento**

Fuente:
Estudio sobre el impacto de la seguridad de API de 2024

Para los organismos gubernamentales, los costes de los ataques de API son elevados: tienen impacto financiero y humano. La pérdida de confianza a nivel de liderazgo debido a las vulneraciones puede suponer un mayor escrutinio, interrupciones operativas y más trabajo para los equipos que ya están limitados y tienen dificultades para satisfacer las exigencias de conformidad.

Akamai

Al igual que en el sector privado, cuesta distinguir entre actividad de API legítima y maliciosa. Esto se debe, en parte, a la escasa visibilidad de los puntos en los que las API son vulnerables. Si bien el 66,9 % de los encuestados afirma que tiene un inventario completo de sus API, solo el 18,5 % de los que lo tienen sabe cuáles incluyen datos confidenciales, como información de identificación personal (documentos de identidad, datos biométricos o información de contacto).

Piense qué pasaría si un departamento o una filial de una organización pública implementa una API no autorizada sin la colaboración o la supervisión de los equipos de seguridad o de TI centrales más actualizados.

Esta API podría:

- Estar diseñada para proporcionar acceso a los datos personales o financieros de los ciudadanos sin controles de autorización adecuados, y exponer información confidencial.
- Haberse actualizado a una nueva versión de forma incorrecta, lo que dejaría terminales obsoletos y vulnerables a explotaciones.
- Operar fuera de la visibilidad de los equipos centrales de TI y seguridad, evadiendo las herramientas de supervisión y las comprobaciones de conformidad normativa tradicionales.
- Explotarse por agentes maliciosos para obtener acceso no autorizado a los sistemas gubernamentales, lo que podría dar lugar a filtraciones de datos, robo de identidad o fraude financiero.

No son solamente hipótesis: el panorama de ciberseguridad para las agencias gubernamentales de EE. UU. presenta importantes desafíos. Según el Cybernews Business Digital Index, a muchas agencias y departamentos gubernamentales les cuesta mantener una seguridad sólida. Más concretamente, 4 de cada 10 (38,8 %) reciben calificaciones de "riesgo crítico" en sus evaluaciones, y el 75 % ha sufrido una filtración de datos.

Estas estadísticas reflejan la compleja realidad a la que se enfrentan los equipos de seguridad gubernamentales, que deben equilibrar los objetivos de sus misiones, los sistemas heredados y las amenazas en constante evolución, al tiempo que operan bajo restricciones y escrutinios únicos. A medida que estos desafíos se intensifican, especialmente en el ámbito de la seguridad de las API, las entidades necesitan partners que comprendan sus requisitos específicos y puedan proporcionar soluciones adaptadas a los entornos gubernamentales.

Impacto de los incidentes de API en la confianza, los costes y el estrés del equipo

Dada la frecuencia y los costes de los ataques a las API, no es de extrañar que proteger las API sea una prioridad cada vez mayor para los gobiernos de todo el mundo. En los Estados Unidos, la iniciativa de Data.gov, gestionada por la Administración General de Servicios, estandariza las API en todos los organismos federales para mejorar la coherencia, la seguridad y la interoperabilidad. Se están realizando esfuerzos similares a nivel mundial, desde marcos de datos abiertos en la Unión Europea y el Reino Unido hasta iniciativas de transformación digital en las regiones de Asia-Pacífico y Oriente Medio, donde los gobiernos están adoptando API estandarizadas para garantizar intercambios de datos seguros y sin interrupciones.

Muchas de estas iniciativas están en consonancia con las normativas regionales, como el RGPD de la UE, el marco Notifiable Data Breaches de Australia y la ley My Number Act de Japón. Mediante la aplicación de estándares y marcos comunes, los gobiernos están trabajando para garantizar un intercambio de datos seguro, al tiempo que reducen los riesgos derivados de integraciones de terceros y accesos no autorizados.

	Sector gubernamental	Media de todos los sectores
Estados Unidos	717 500,50 USD	591 404,01 USD
Reino Unido	378 140,69 GBP	420 103,18 GBP
Alemania	296 975,79 EUR	403 453,26 EUR

P3. Si ha sufrido algún incidente de seguridad de API, ¿cuál ha sido el impacto financiero total estimado de estos incidentes combinados? Incluya todos los costes relacionados, como reparaciones del sistema, tiempo de inactividad, honorarios legales, multas y cualquier otro gasto asociado.

Está claro que las entidades gubernamentales son plenamente conscientes de las consecuencias que tienen las amenazas de las API. Por primera vez, solicitamos a los encuestados de los tres países participantes que divulgaran el impacto financiero estimado de los incidentes de seguridad de las API que han experimentado en los últimos 12 meses.

Si bien las repercusiones financieras son significativas, los participantes del estudio afirmaron con rotundidad que los costes no solo afectan a los resultados empresariales.

Cuando se les pidió que enumeraran las principales consecuencias de un incidente de seguridad de API, estas no eran de carácter económico. Como se mencionó anteriormente, nuestros encuestados resaltaron sobre todo el "aumento del estrés o la presión para el equipo o el departamento" y los "daños a la reputación de nuestro departamento ante los altos puestos y la junta directiva".

Estas consecuencias dejan un impacto duradero. Las vulneraciones erosionan la confianza, lo que puede poner en peligro la financiación futura y debilitar la veracidad percibida. Al mismo tiempo, las pérdidas de productividad en entidades ya limitadas pueden provocar agotamiento y reducir el compromiso de los empleados.

Pero la presión no se limita a unas pocas regiones. Aunque este informe se centra en determinados mercados, la seguridad de las API se ha convertido en un problema crítico para las organizaciones del sector público de todo el mundo, ya que los organismos de Asia-Pacífico, Latinoamérica y otros países se enfrentan a retos similares a la hora de proteger la infraestructura digital, cumplir los estándares normativos y proteger los datos confidenciales ante amenazas en constante evolución.

Reducción del riesgo y el estrés mediante la seguridad proactiva de API

Los ataques a las API dirigidos a gobiernos están aumentando de alcance, escala, sofisticación y coste. Esto incluye los ataques de bots impulsados por IA generativa, que se adaptan rápidamente para eludir las herramientas de seguridad de API tradicionales y otras defensas perimetrales. Muchos equipos de seguridad de su sector están experimentando estas amenazas de primera mano y padecen las consecuencias, tanto en términos financieros como humanos. Con todo, incluso cuando las organizaciones comprenden la importancia de las amenazas de API, se plantean la siguiente pregunta: ¿Qué podemos hacer?

Tomar medidas ya para proteger mejor sus API, así como los datos que intercambian, puede permitir a su organización proteger sus ingresos y los datos confidenciales, y aliviar la carga de los equipos de seguridad; todo ello al tiempo que se mantiene la confianza que tanto les ha costado ganarse de las juntas directivas y los responsables gubernamentales. Entre estos medidas se incluye el desarrollo de los conocimientos de su equipo sobre las amenazas de API avanzadas y las capacidades necesarias para defenderse ante ellas.

Para leer el informe completo y obtener más información sobre las prácticas recomendadas en materia de visibilidad y protección de API, descargue el **Estudio sobre el impacto de la seguridad de API de 2024**.

¿Todo listo para hablar sobre sus retos y descubrir cómo puede ayudarle Akamai?

Solicite una demostración personalizada de la solución Akamai API Security

Akamai

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Aprovechando la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn. Publicado el 25 de mayo.