ESTUDIO SOBRE EL IMPACTO DE LA SEGURIDAD DE LAS API DE 2024

Sector de la atención sanitaria

Los incidentes relacionados con las API aumentan. Descubra cómo el sector de la asistencia sanitaria está afrontando los desafíos de seguridad de las API y qué puede hacer para defenderse de las amenazas en constante evolución.

En un sector en el que la confianza de los pacientes y los afiliados resulta esencial, las organizaciones sanitarias se enfrentan a un desafío de seguridad cada vez mayor: las vulnerabilidades de las API.

Los historiales médicos electrónicos, los servicios de videoconsulta y los dispositivos médicos conectados se han convertido en el objetivo principal de los ciberdelincuentes. Además, la información sanitaria protegida (PHI) a la que se accede a través de API no seguras puede provocar infracciones de la HIPAA, poner en peligro la privacidad de los pacientes y empañar una confianza que se tarda años en restablecer.

La magnitud de este problema es bastante considerable. En la exhaustiva encuesta de Akamai, un alarmante 84,7 % de los profesionales sanitarios hablaron de incidentes relacionados con la seguridad de las API durante el último año, porcentaje ligeramente superior a la media del 84 % en todos los sectores.

Sin embargo, tal vez lo más preocupante sea el impacto en la confianza: los encuestados del sector sanitario afirman que la "pérdida de la confianza y la reputación" (28,7 %) es una de sus principales preocupaciones tras los incidentes que afectaron a las API. En un mundo en el que los pacientes pueden cambiar fácilmente de proveedor, este daño a la reputación puede tener efectos a largo plazo que van más allá de los costes inmediatos.

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

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

El coste financiero de los ataques a las API es considerable, ya que las organizaciones del sector sanitario gastan una media de 510 600 dólares en solucionar estos incidentes.

A pesar de estos riesgos, los datos revelan que existe una preocupante discrepancia con respecto a las prioridades. Cuando se les preguntó sobre cuáles eran sus principales prioridades relacionadas con la ciberseguridad para los siguientes 12 meses, las organizaciones de atención médica colocaron "proteger las API de los atacantes" en el puesto 11 (16,7 %) de los 12 existentes. Esta organizaciones se están concentrando más en garantizar la autenticación del personal que accede a los sistemas (24,7 %) y en gestionar los secretos de los desarrolladores (22,7 %).

La distinción entre la actividad de las API legítima y maliciosa sigue siendo un reto para los proveedores de atención sanitaria. Si bien el 65 % de los profesionales del sector afirman contar con inventarios de API exhaustivos, solo el 24 % de ese subgrupo conocen cuáles de esas API gestionan datos confidenciales, lo que supone un preocupante descenso con respecto al 40 % registrado en 2023. En la atención sanitaria, donde la privacidad de los datos no es solo una buena práctica sino un requisito legal, esta brecha en la visibilidad representa un importante riesgo.

Piense en lo que puede suceder con una API que implemente un departamento clínico sin una supervisión adecuada por parte de los equipos centrales de seguridad o TI. Esta API podría:

- Diseñarse para compartir historiales de pacientes sin los controles adecuados que cumplan con la HIPAA.
- Quedarse activa después de realizar actualizaciones en el sistema, lo que generaría puntos de acceso desconocidos.
- Pasar desapercibida para herramientas de seguridad tradicionales que no se hayan diseñado para detectar API no gestionadas.
- Utilizarse por parte de los atacantes para acceder a información sanitaria protegida.
- Utilizarse de forma indebida por un partner legítimo, que utilice el terminal para fines no intencionados.

84,7 % de las organizaciones sanitarias han sufrido incidentes de las API en los últimos 12 meses.

65 % de las organizaciones sanitarias tienen inventarios completos de API, pero de todas ellas, solo el 24 % saben cuáles incluyen datos confidenciales.

510 600 $ es el impacto financiero que han representado los incidentes de seguridad de las API para las organizaciones sanitarias en los últimos 12 meses.

3 consecuencias principales

1. **Pérdida de la confianza y la reputación** (28,7 %)
2. **Pérdida de productividad** (28,7 %)
3. **Mayor escrutinio interno** (27,3 %)

Fuente:
Akamai, "Estudio sobre el impacto de la seguridad de API", 2024

Akamai

Esto no es una mera hipótesis. Con las filtraciones de datos en el sector sanitario que alcanzan máximos históricos y los costes de filtración de datos que alcanzan, de media, 4,88 millones de dólares[1] por incidente, las vulnerabilidades de las API representan un riesgo de seguridad y cumplimiento cada vez mayor. Además, este escenario refleja lo que las empresas de su sector citan como las principales causas de sus incidentes de API.

Impacto de los incidentes de API en el cumplimiento, los costes empresariales y el estrés del equipo

Así lo expone el informe Gartner® Market Guide for API Protection de mayo de 2024[2]: "Según datos actuales, se estima que cada vez que se vulnera una API, se filtran de media 10 veces más datos confidenciales que con cualquier otro tipo de incidente".

No es de extrañar que el cumplimiento de la ley HIPAA exija centrarse cada vez más en la seguridad de las API. Aunque esta ley no menciona explícitamente las API, exige que se restrinja el acceso a la PHI según las funciones de los empleados. Para ello es necesario contar con controles de acceso y autenticación en las API que transmitan información de pacientes. Los proveedores de atención sanitaria y las aseguradoras, así como sus reguladores, necesitan saber qué tipos de datos se transmiten, no solo a través de sus propias API, sino también mediante las API de sus partners y proveedores, lo que añade otro reto a la gestión del riesgo de terceros en el sector de la atención sanitaria.

La pérdida de la confianza de los reguladores puede resultar en un mayor escrutinio, lo que a su vez supondría más trabajo para los equipos, que ya atraviesan dificultades para satisfacer las exigencias en materia de cumplimiento. Además, esto podría acarrear la imposición de multas cuantiosas. Teniendo estos datos en cuenta, no cabe duda de que las empresas de atención sanitaria son plenamente conscientes de las consecuencias financieras de las amenazas de API. Por primera vez, solicitamos a los encuestados de los tres países participantes que divulgaran los costes estimados de los incidentes de seguridad de las API que han experimentado en los últimos 12 meses.

	Sector de la atención sanitaria	Media de todos los sectores
EE. UU.	510 600 $	591 404 $
Reino Unido	363 885 £	420 103 £
Alemania	643 884 €	403 453 €

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.

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 el impacto principal de un incidente de seguridad de API, este no era de carácter económico. Como se ha mencionado anteriormente, nuestros encuestados hicieron hincapié en la "pérdida de la confianza y la reputación" (28,7 %) y la "pérdida de productividad" (28,7 %). Estas consecuencias pueden tener efectos duraderos: una menor confianza de los pacientes puede perjudicar los ingresos de los años futuros, mientras que la pérdida de productividad en el ya de por sí sobrecargado personal sanitario puede aumentar su agotamiento y desmotivación.

[1] IBM Cost of a Data Breach Report (Informe de IBM sobre el coste de la vulneración de datos), 2024

[2] Gartner, Market Guide for API Protection, 29 de mayo de 2024. GARTNER es una marca comercial registrada y una marca de servicio de Gartner, Inc. y/o sus filiales en EE. UU. y otros países, y se usa aquí con permiso. Todos los derechos reservados.

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

Los ataques a las API dirigidos a empresas del sector sanitario 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 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 clientes. Entre estos pasos 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

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 marzo.