ESTUDO SOBRE O IMPACTO DA SEGURANÇA DE APIS DE 2024

Setor de saúde

Os incidentes de API estão aumentando. Saiba como o setor de saúde está lidando com os desafios de segurança de APIs e o que você pode fazer para se defender contra as ameaças crescentes.

Em um setor em que a confiança do paciente e dos membros é primordial, as organizações de saúde enfrentam um desafio de segurança crescente: vulnerabilidades de APIs.

Prontuários médicos eletrônicos, telemedicina e dispositivos médicos conectados tornaram-se alvos para os cibercriminosos, e informações de saúde confidenciais (PHI) acessadas por APIs não protegidas podem levar a violações da HIPAA, privacidade comprometida do paciente e danos à confiança, que leva anos para ser reconstruída.

A escala desse desafio é significativa. Na pesquisa abrangente da Akamai, um número alarmante de 84,7% dos profissionais de saúde relatou incidentes de segurança de APIs no último ano, um pouco maior que a média de 84% entre setores.

Mas talvez o mais preocupante seja o impacto na confiança: Os entrevistados da área de saúde relatam "perda de confiança e reputação" (28,7%) como uma das principais preocupações após incidentes com APIs. Em um mundo onde os pacientes podem facilmente mudar de fornecedor, esse dano reputacional pode ter efeitos duradouros além dos custos imediatos.

Continue lendo para obter insights do setor a partir do Estudo sobre o impacto da segurança de APIs de 2024.

À medida que ataques aumentam, a visibilidade é uma preocupação crescente

O valor financeiro dos ataques contra APIs é substancial, com organizações de saúde gastando em média US$ 510.600 para lidar com esses incidentes.

Apesar dos riscos, os dados revelam uma lacuna preocupante nas prioridades. Quando questionadas sobre suas principais prioridades de cibersegurança nos próximos 12 meses, as organizações de saúde classificaram a "proteção de APIs contra agentes de ameaça" em 11º lugar (16,7%) entre 12 opções. Em vez disso, elas estão se concentrando em proteger a autenticação para a equipe que acessa os sistemas (24,7%) e em gerenciar os segredos do desenvolvedor (22,7%).

Distinguir entre atividade de API legítima e mal-intencionada ainda é um desafio para os profissionais de saúde. Embora 65% de seus colegas relatem ter inventários completos de API, apenas 24% desse subconjunto sabe quais APIs lidam com dados confidenciais, uma queda preocupante em relação aos 40% registrados em 2023. Para a área da saúde, onde a privacidade de dados não é apenas uma boa prática, mas uma lei, essa lacuna de visibilidade cria um risco significativo.

Considere o que pode acontecer com uma API implantada por um departamento clínico sem a supervisão adequada das equipes centrais de TI ou segurança. Essa API pode ter sido:

- Criada para compartilhar prontuários sem controles adequados em conformidade com a HIPAA
- Deixada ativa após as atualizações do sistema, criando pontos de acesso desconhecidos
- Ignorada por ferramentas de segurança tradicionais não projetadas para detectar APIs não gerenciadas
- Explorada por invasores para acessar informações de saúde protegidas
- Utilizada por um parceiro autêntico, usando o endpoint para casos de uso não intencionais

84,7% das organizações de saúde sofreram incidentes de API nos últimos 12 meses

65% das organizações de saúde têm inventários de API completos, mas, entre elas, apenas 24% sabem quais APIs retornam dados confidenciais

US$ 510.600 = impacto financeiro de incidentes de segurança de APIs para organizações de saúde nos últimos 12 meses

Os três principais impactos

1. **Perda de confiança e reputação** (28,7%)
2. **Perda de produtividade** (28,7%)
3. **Aumento do escrutínio interno** (27,3%)

Fonte:
Akamai, "Estudo sobre o impacto da segurança de APIs", 2024

Akamai

Esta não é apenas uma história hipotética. Com as violações de dados da área da saúde atingindo altos recordes e os custos de violação de dados em uma média de US$ 4,88 milhões[1], as vulnerabilidades de API representam um risco crescente de conformidade e segurança. Além disso, esse cenário reflete o que seus colegas citam como as principais causas de seus incidentes de API.

Como os incidentes de API afetam a conformidade, o custo para a empresa e o estresse da equipe

De acordo com o Market Guide for API Protection de maio de 2024[2] da Gartner®, "os dados atuais indicam que a violação média de APIs leva a pelo menos 10 vezes mais dados vazados do que a violação média de segurança".

Não é de se admirar que as exigências de conformidade com a HIPAA se concentrem cada vez mais na segurança de APIs. Embora a HIPAA não mencione explicitamente as APIs, ela exige a restrição do acesso às PHIs com base nas funções de cada funcionário. Isso requer controles de autenticação e acesso em APIs que transmitem dados do paciente. Os provedores e operadoras de planos de saúde — e seus reguladores — precisam saber quais tipos de dados estão transitando não apenas por suas próprias APIs, mas também pelas APIs de seus parceiros e fornecedores, adicionando mais um desafio ao gerenciamento de riscos de terceiros para o setor de saúde.

Perder a confiança dos reguladores pode resultar em maior escrutínio e mais trabalho para equipes que estão sobrecarregadas lutando para atender às demandas de conformidade. Isso também pode resultar em multas elevadas. Pensando nisso, fica claro que as empresas de saúde estão profundamente cientes das consequências financeiras das ameaças de API. Pela primeira vez, pedimos aos entrevistados nos três países pesquisados que compartilhassem os custos estimados dos incidentes de segurança de APIs que vivenciaram nos últimos 12 meses.

	Setor de saúde	Média de todos os setores
EUA	US$ 510.600	US$ 591.404
Reino Unido	£ 363.885	£ 420.103
Alemanha	€ 643.884	€ 403.453

P3. Se você sofreu um incidente de segurança de APIs, qual foi o impacto financeiro total estimado da combinação desses incidentes? Inclua todos os custos relacionados, como reparos no sistema, tempo de inatividade, taxas legais, multas e quaisquer outras despesas associadas.

Embora os impactos financeiros sejam significativos, ouvimos em alto e bom som dos participantes do estudo que os custos vão muito além disso. O custo não foi o item principal citado quando pedimos para listar o principal impacto de um incidente de segurança de APIs. Como mencionado anteriormente, nossos entrevistados enfatizaram a "perda de confiança e reputação" (28,7%) e a "perda de produtividade" (28,7%). Essas consequências têm efeitos duradouros; a confiança do paciente prejudicada pode impactar a receita dos anos futuros, enquanto as perdas de produtividade de profissionais de saúde já sobrecarregados podem acelerar o esgotamento e o descomprometimento da equipe.

[1] Relatório IBM: Custo de uma violação de dados (em inglês), 2024

[2] Gartner, Market Guide for API Protection, 29 de maio de 2024. GARTNER é uma marca registrada e marca de serviço da Gartner, Inc. e/ou de suas afiliadas nos EUA e internacionalmente, e é usada aqui com permissão. Todos os direitos reservados.

Reduza o risco e o estresse com a segurança de APIs proativa

Os ataques de API contra empresas de saúde estão crescendo em escopo, escala, sofisticação e custo. Isso inclui ataques de bots alimentados por IA generativa que se adaptam rapidamente para contornar as ferramentas tradicionais de segurança de APIs e outras defesas de perímetro. Muitas equipes de segurança do seu setor estão vivenciando essas ameaças em primeira mão e sentindo os impactos, tanto financeiros quanto humanos. Porém, mesmo quando as organizações entendem a importância das ameaças de API, elas ficam com a dúvida: *o que podemos fazer a respeito disso?*

Tomar medidas agora para proteger melhor suas APIs (e os dados que elas trocam) pode capacitar sua organização a proteger sua receita e aliviar o fardo das equipes de segurança, tudo isso preservando a confiança arduamente conquistada de conselhos de administração e clientes. Essas etapas incluem o desenvolvimento do conhecimento da equipe sobre ameaças avançadas de APIs e os recursos necessários para se defender contra elas.

Para ler o relatório completo e saber mais sobre as práticas recomendadas de visibilidade e proteção de APIs, faça o download do **Estudo sobre o impacto da segurança de APIs de 2024**.

Pronto para conversar sobre seus desafios e como a Akamai pode ajudar?

Solicite uma demonstração personalizada do Akamai API Security

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem comprometer o desempenho ou a experiência do cliente. Ao aproveitar a escala de nossa plataforma global e sua visibilidade de ameaças, trabalhamos com você para evitar, detectar e mitigar ameaças, permitindo que você construa a confiança na sua marca e opere de acordo com a sua visão. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em akamai.com e akamai.com/blog ou siga a Akamai Technologies no X e LinkedIn. Publicado em 03/25.