ESTUDO SOBRE O IMPACTO DA SEGURANÇA DE APIS DE 2024

Setor de serviços financeiros

Os incidentes de API estão aumentando. Descubra como o setor de serviços financeiros está enfrentando essa grande preocupação com a segurança e o que sua organização pode fazer para se proteger.

No ano passado, 88,7% das empresas de serviços financeiros foram alvo de ataques a APIs que gerenciam seus dados e conectam clientes e parceiros a serviços essenciais. Usando métodos cada vez mais sofisticados, agentes de ameaça podem explorar APIs desprotegidas para acessar dados e roubar informações pessoais e financeiras, incluindo saldos de contas e históricos de transações.

As equipes de segurança estão enfrentando os impactos e buscando formas de aprimorar suas estratégias. Lidar com mais um vetor de ataque pode parecer desafiador, especialmente quando se trata de APIs, cujas configurações incorretas ou falhas de lógica de negócios podem ser facilmente identificadas e exploradas.

Como sabemos disso? A Akamai entrevistou mais de 1.200 profissionais de TI e segurança, desde diretores de segurança da informação até equipes de segurança de aplicativos, para entender suas experiências com ameaças relacionadas a APIs.

Aqui, filtramos nossas descobertas para os entrevistados do setor de serviços financeiros, que apontaram como principais impactos de seus incidentes de segurança em APIs as "multas de órgãos reguladores" e o "aumento do estresse e/ou pressão sobre minha equipe ou departamento". Essas consequências são fáceis de compreender, já que seus colegas relataram que o custo para lidar com incidentes de API foi de US$ 832.800 – 40% superior à média dos oito setores pesquisados e o mais alto entre todos os setores.

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

A visibilidade está diminuindo à medida que os ataques aumentam

Embora 84% das organizações de todos os setores tenham enfrentado incidentes de segurança em APIs, as empresas de serviços financeiros foram atacadas com mais frequência do que a média, atingindo 88,7%. Seus colegas apontaram duas vulnerabilidades principais que impulsionam esses ataques: a incapacidade dos firewalls de rede de detectar ameaças (26,5%) e as vulnerabilidades em APIs de ferramentas de IA generativa, como modelos de linguagem grandes (LLMs) (23,2%).

Apesar das evidências crescentes sobre as ameaças às APIs, incluindo incidentes frequentes, altos custos de correção e multas regulatórias, nossas descobertas indicam que muitas equipes do setor de serviços financeiros ainda não priorizaram a segurança das APIs. Na verdade, a segurança de API ocupa o nono lugar entre as prioridades de cibersegurança no ano seguinte, em 18,5%.

A diferenciação entre atividade legítima e maliciosa ou fraudulenta em APIs continua sendo um desafio para o setor financeiro, especialmente no que diz respeito à visibilidade dos diversos riscos associados às APIs. Embora 73,5% de seus colegas afirmem ter um inventário completo de suas APIs, apenas 28,5% desse grupo sabem quais delas retornam dados confidenciais, incluindo informações de identificação pessoal (PII) e dados que vão desde históricos de crédito de titulares de cartão até registros financeiros de grandes clientes de serviços bancários comerciais.

88,7% das empresas do setor financeiro sofreram um incidente de segurança de API nos últimos 12 meses

Apenas 28,5% das empresas do setor financeiro com inventários completos de APIs sabem quais APIs retornam dados confidenciais

US$ 832.800 = Impacto financeiro dos incidentes de segurança em APIs para empresas de serviços financeiros que os enfrentaram nos últimos 12 meses

Os três principais impactos

1. **Aumento do estresse e/ou da pressão** sobre a equipe de segurança
2. **Multas** dos reguladores
3. **Perda de confiança** e reputação

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

Akamai

Imagine o que pode acontecer com uma API shadow implantada por um departamento ou subsidiária de um provedor de serviços financeiros sem a colaboração ou supervisão das equipes centrais de TI ou segurança da empresa. Essa API pode ter sido:

- Criada para retornar dados de transações dos clientes sem os devidos controles de autorização e sem ter sido testada adequadamente para identificar configurações incorretas
- Substituída por uma nova versão, mas não desativada, permanecendo assim exposta à Internet
- Ignorada pelo radar das ferramentas tradicionais que não conseguem detectar APIs não gerenciadas
- Explorada por criminosos que acessam contas de clientes reais para roubar seus ativos

Esta não é apenas uma história hipotética. De acordo com o estudo True Cost of Fraud™ 2023 da LexisNexis® Risk Solutions, 50% das perdas por fraude podem ser atribuídas ao abuso na abertura de novas contas, onde fraudadores exploram indevidamente APIs para criar contas em grande escala. Além disso, nosso cenário reflete o que a TI e a segurança da vida real 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 da Gartner®*, "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 surpresa que a regulamentação PCI DSS v4.0, amplamente adotada, tenha incorporado novos requisitos relacionados à segurança de APIs. O padrão agora exige que as organizações validem seu código de API antes do lançamento, testem regularmente vulnerabilidades e garantam o uso seguro de componentes baseados em API, algo especialmente importante em um setor onde as APIs viabilizam milhões de transações financeiras todos os dias.

Perder a confiança dos reguladores pode levar a um escrutínio mais rigoroso e a uma carga de trabalho ainda maior para equipes já sobrecarregadas, que lutam para atender às exigências de conformidade. Isso também pode levar à aplicação de multas elevadas.

Pensando nisso, fica claro que as empresas do setor financeiro estão profundamente cientes das consequências financeiras das ameaças às APIs. Pela primeira vez, solicitamos aos entrevistados dos três países pesquisados que compartilhassem a estimativa do impacto financeiro causado pelos incidentes de segurança em APIs que enfrentaram nos últimos 12 meses.

	Setor de serviços financeiros	Média de todos os setores
EUA	US$ 832.800	US$ 591.404
Reino Unido	£ 297.189	£ 420.103
Alemanha	€ 604.405	€ 403.453

P3. Se sua organização enfrentou um incidente de segurança em APIs, qual foi a estimativa do impacto financeiro total resultante da soma desses incidentes? Inclua todos os custos relacionados, como reparos no sistema, tempo de inatividade, honorários legais, multas e quaisquer outras despesas associadas.

* 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 a APIs de empresas do setor financeiro estão crescendo em escopo, escala, sofisticação e custo. Isso inclui ataques de bots impulsionados 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 enfrentando essas ameaças diretamente e sentindo seus impactos, tanto financeiros quanto operacionais. Porém, mesmo quando as organizações entendem a importância das ameaças a APIs, elas ficam com a dúvida: o que podemos fazer a respeito disso?

Tomar medidas agora para fortalecer a segurança de suas APIs e dos dados que elas trocam pode ajudar sua organização a proteger sua receita e reduzir a carga das equipes de segurança. Essas medidas, aliadas ao fortalecimento do conhecimento da sua equipe sobre ameaças avançadas a APIs e aos recursos necessários para combatê-las, podem ajudar a preservar a confiança que você conquistou de clientes e conselhos de administração.

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

A Akamai oferece soluções desenvolvidas para ajudar as organizações a mitigar os riscos associados às ameaças discutidas nesta seção:

- O Akamai API Security identifica APIs, avalia sua postura de risco, analisa seu comportamento e impede que ameaças se ocultem dentro delas.
- O Akamai Account Protector ajuda a prevenir o abuso na abertura de contas ao monitorar o comportamento do usuário em tempo real e se adaptar às mudanças nos perfis de risco.

Akamai

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem prejudicar o desempenho ou a experiência do cliente. Ao utilizar a escala de nossa plataforma global e sua ampla visibilidade de ameaças, trabalhamos com você para prevenir, detectar e mitigar riscos, permitindo que sua marca fortaleça a confiança e opere de acordo com 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.