ESTUDO SOBRE O IMPACTO DA SEGURANÇA DE APIs DE 2024

Indústria de varejo e comércio eletrônico

Como seus colegas veem e vivenciam a crescente ameaça às APIs

As APIs que sustentam as iniciativas digitais das empresas de varejo e comércio eletrônico estão sob ataque. Usando métodos cada vez mais inovadores, os agentes de ameaças podem acessar dados em APIs desprotegidas para roubar dados de cartão de crédito, desviar fundos de programas de fidelidade, lançar ataques de preenchimento de credenciais e muito mais. As equipes de segurança estão sentindo o impacto e buscando maneiras de melhorar. Enfrentar outro vetor de ataque pode parecer assustador, especialmente um como as APIs, cujas configurações incorretas ou falhas de lógica comercial podem ser facilmente descobertas e exploradas.

Como sabemos disso? A Akamai pesquisou mais de 1.200 profissionais de TI e segurança, de CISOs a equipes de AppSec, para saber mais sobre suas experiências com ameaças relacionadas a APIs.

Este estudo filtra essas descobertas para o seu setor, onde 68% dos entrevistados relataram ter sofrido incidentes de segurança de API nos últimos 12 meses. Quais foram os impactos? As principais respostas dos seus colegas incluíram o aumento dos níveis de estresse das equipes e a perda de credibilidade entre os executivos seniores e as diretorias. Essa resposta é compreensível, dados os custos relatados, uma vez que os profissionais de varejo e comércio eletrônico mencionaram um valor de US$ 526.531,00 para lidar com os incidentes de API que sofreram.

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

Enquanto os ataques aumentam, a visibilidade diminui

Embora uma maioria notável dos entrevistados do setor de varejo e comércio eletrônico tenha sofrido incidentes de segurança de API, a média de 68% foi inferior aos 84% relatados em todos os oito setores pesquisados. Enquanto isso, as principais prioridades de segurança de seus colegas do setor para os próximos 12 meses são "defesa contra ataques alimentados por IA generativa" e "proteção de APIs contra agentes de ameaças".

Existe uma ligação entre priorizar APIs e prevenir ataques? É possível que as equipes de segurança das empresas de varejo e comércio eletrônico tenham reconhecido a importância da proteção das APIs e que seus esforços estejam reduzindo os incidentes. No entanto, nossas descobertas também sugerem que essas equipes não estão vendo todos os casos de abuso de APIs.

Distinguir entre atividade de API genuína e maliciosa ou fraudulenta permanece desafiador para empresas de varejo e comércio eletrônico. A visibilidade do risco também é um desafio. Enquanto 67% dos seus pares do setor relatam ter inventários de API completos, *apenas 29%* desse subgrupo sabe qual das suas inúmeras APIs retornam dados confidenciais. Isso inclui PII (informações de identificação pessoal) ou detalhes do cartão de crédito.

Considere o que pode acontecer com uma API implantada por uma unidade de negócios sem a colaboração ou a supervisão das equipes centrais de TI ou de segurança do varejista. Essa API pode ter sido:

- Criada para retornar os dados dos clientes sem os devidos controles de autorização e não testada adequadamente quanto a 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 fraudadores que acessam contas de fidelidade de clientes reais e resgatam dinheiro

68% das empresas de varejo/comércio eletrônico sofreram um incidente de segurança de API nos últimos 12 meses[1]

Apenas 29% das empresas de varejo/comércio eletrônico com inventários completos de APIs sabem quais APIs retornam dados confidenciais[1]

US$ 526.531 = impacto financeiro dos incidentes de segurança de API para empresas de varejo/comércio que os sofreram nos últimos 12 meses[1]

Os três principais impactos[1]

1. **Aumento do estresse** e/ou da pressão para minha equipe
2. **Custos gerados** para ajudar a corrigir o problema
3. **Danos à reputação do departamento** diante de líderes seniores e/ou o conselho de diretores

44% dos ataques na Web contra organizações comerciais tiveram como alvo as APIs[2]

Fontes:
1. Akamai, "Estudo sobre o impacto da segurança de APIs", 2024
2. Akamai State of the Internet (SOTI), "Escondido nas sombras: Tendências de ataque trazem à tona ameaças a APIs", 2024

Akamai

Esta não é apenas uma história hipotética. De acordo com o estudo True Cost of Fraud™ de 2023 da LexisNexis® Risk Solutions, 50% das perdas por fraude podem ser atribuídas ao abuso de abertura de novas contas, em que os fraudadores usam indevidamente as APIs para abrir contas em 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.

Principais causas de incidentes de API citadas pelas equipes de segurança de varejo/comércio eletrônico

1. APIs em ferramentas de IA generativas, por exemplo, LLMs – **24,7%**
2. API com exposição não intencional na Internet – **24%**
3. Configuração incorreta da API – **22%**
4. O firewall de aplicativos da Web não detectou o problema – **21,3%**
5. O gateway da API não detectou o problema – **20,7%**
6. Vulnerabilidade devido a erros de codificação da API – **20%**
7. Uma ferramenta/serviço de tecnologia bem conhecida – **20%**
8. O firewall de rede não detectou o problema – **18,7%**
9. Vulnerabilidades de autorização – **17,3%**
10. Solução de software descarregada da internet – **16,7%**
11. Falta de controles de autenticação de API – **16%**
12. Solução de software de nível médio – **14,7%**
13. APIs não gerenciadas (por exemplo, zumbi) – **13,3%**

P. Em sua opinião, quais são as causas dos incidentes de segurança de APIs que sua organização sofreu? (Selecione até 3) n=1.207

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

De acordo com o Gartner® Market Guide for API Protection, de maio de 2024, "os dados atuais indicam que a violação média da API leva a um vazamento de dados pelo menos 10 vezes maior do que a violação média de segurança".[3] Não é de se admirar que a regulamentação PCI DSS v4.0, amplamente seguida, tenha acrescentado requisitos relativos à segurança da API. As empresas e seus reguladores precisam saber quais tipos de dados estão trafegando não apenas por suas próprias APIs, mas também pelas APIs de seus parceiros e fornecedores, acrescentando mais um desafio ao gerenciamento de riscos de terceiros para o comércio eletrônico.

Perder a confiança dos órgãos reguladores pode resultar em maior fiscalização e mais trabalho para equipes sobrecarregadas que lutam para atender às demandas de conformidade. Isso também pode resultar em multas elevadas. E com os custos em mente, fica claro que as empresas de varejo e comércio eletrônico estão bem cientes das consequências financeiras das ameaças a APIs. Pela primeira vez, pedimos aos entrevistados nos três países pesquisados que compartilhassem o impacto financeiro estimado dos incidentes de segurança de API que sofreram nos últimos 12 meses.

[3] 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.

	Varejo/comércio eletrônico	Média de todos os setores
US	US$ 526.531	US$ 591.404
Reino Unido	£ 258.815	£ 420.103
Alemanha	€ 348.467	€ 403.453

P. 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. n=1.207

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 os entrevistados foram solicitados a listar o principal impacto de um incidente de segurança de APIs. Nossos entrevistados do setor de varejo e comércio eletrônico enfatizaram o custo humano: estresse e pressão sobre suas equipes.

Os cinco principais impactos dos incidentes de segurança de API para empresas de varejo e comércio eletrônico

1. Aumentou o estresse e/ou a pressão para minha equipe/departamento – **28,7%**

2. Custos incorridos para ajudar a corrigir o problema – **28%**

3. Danos à reputação do departamento diante dos nossos líderes seniores e/ou o conselho de diretores – **25,3%**

4. Levou a um maior escrutínio interno da nossa equipe/departamento pela empresa – **23,3%**

5. Multas regulatórias – **25,3%**

P. Quais custos e/ou impactos, se houver, os incidentes com a segurança de APIs tiveram em sua empresa? (Selecione até 3) n=1.207

Próximos passos: reduza o risco e o estresse com a segurança proativa para as APIs

Os ataques de API contra empresas de varejo e comércio eletrônico estão crescendo em escopo, escala e sofisticação. 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?

Adotar medidas agora para proteger melhor as APIs, e os dados que elas trocam, pode capacitar a organização a proteger sua receita e aliviar a carga das equipes de segurança, preservando a confiança arduamente conquistada junto aos 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

Akamai

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, antigo Twitter, e LinkedIn. Publicado em 24/11.